Das Internet der Dinge – Die Kontrolle über alles und jeden

In Zukunft sollen alle Gegenstände digital miteinander vernetzt werden – theoretisch sogar Menschen!

Seite 50

Überwachung und Entmündigung durch moderne Autos

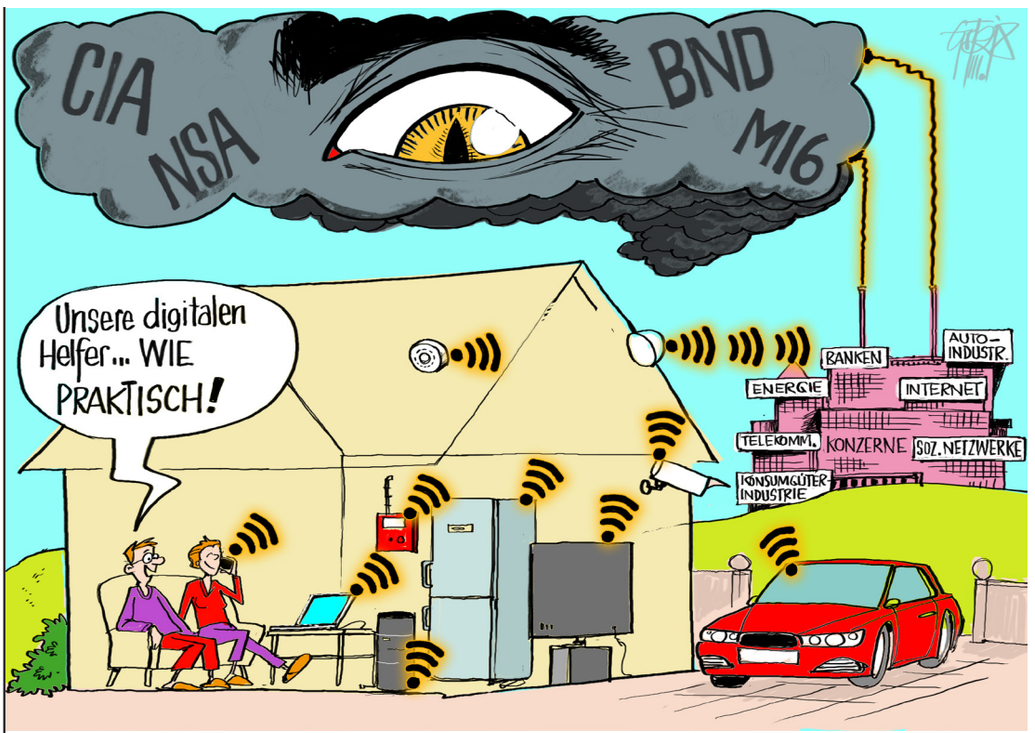
Das Auto der Zukunft soll dem Fahrer jegliche Eigenverantwortung nehmen und automatisch von einem Bordcomputer gesteuert werden.

Seite 32

EXPRESSZEITUNG

Ausgabe 15, März 2018

Jetzt abonnieren - Seite 2



Digitale Überwachung

Aus Bequemlichkeit in die Tyrannei

Wurden Menschen früher noch von ihren Nachbarn und Überwachungskameras bespitzelt, hat beim Thema Überwachung mittlerweile ein einschneidender Paradigmenwechsel stattgefunden: Und zwar vom Zwang zur Freiwilligkeit, von der Nötigung zum Bedürfnis und von der Heimlichkeit zur Offenheit. Eine Überwachung, vor der sich jeder zu drücken versucht, wurde in eine Nachfrage verwandelt. Inzwischen steht der moderne Mensch Schlange für seine Wanzen: Ob das nun Smartphones, Computer oder elektronische Assistenten für zu Hause sind. Die flächendeckende Verwanzung der Erdbevölkerung mit mobilen Luxuswanzen vom Typ Iphone, Samsung Galaxy oder Amazon Echo würde kein Staat und keine internationale Organisation logistisch und finanziell hinbekommen, wenn die Verbraucher das nicht selbst besorgen würden.

Meinungskontrolle durch Google, Facebook, Amazon & Co.

Internetunternehmen kennen die Vorlieben ihrer Nutzer oft besser als ihr Umfeld.

Seite 11

RFID-Technologie: Eine Zukunft ohne Geheimnisse?

RFID-Chips könnten die Position eines jeden Menschen und dessen Interaktion mit Gegenständen rund um die Uhr überwachen.

Seite 20

Dauerüberwachung durch das digitale Stromnetz?

Die neuen digitalen Stromzähler erlauben den Stromkonzernen, jedes Gerät in Ihrem Haus zu überwachen.

Seite 42

Täuschen Sie sich nicht. Wir haben die Möglichkeit, Ihre Haushalte durch Ihre Geräte zu überwachen. Und wenn wir die Möglichkeit haben, dann werden wir sie wahrscheinlich auch nutzen.»

David Howell Petraeus, von 2011 bis 2012 Direktor der CIA

Wir als Menschheit sind den Genies, Erfindern und Vordenkern der letzten 200 Jahre zu unendlichem Dank verpflichtet. Ohne die von ihnen erreichten technischen Quantensprünge wäre der Durchschnittsmensch bis heute, mit einer durchschnittlichen Lebenserwartung von 35 Jahren, auf einer Fläche von wenigen Quadratkilometern gefangen.

In der Tat konnte sich die Menschheit ihrer bisherigen Probleme nur durch Logik und Wissenschaft entledigen. Ärzte forschten nach den Ursachen von Krankheiten und fanden die entsprechenden Gegenmittel. Clevere Tüftler fanden neue Methoden der Energieerzeugung und der Fortbewegung. Die Entwicklung einer elektronischen Rechenmaschine führte zur globalen Vernetzung von über sieben Milliarden Menschen. Heute scheint die Menschheit die wichtigsten Lösungen für fast alle Probleme gefunden zu haben: Der westliche Normalbürger genießt spätestens seit den 60er-Jahren den Lebensstandard eines Königs aus dem Mittelalter.

Doch verwirrenderweise scheint dieser Fortschritt seit einer Weile für den Normalbürger aufgehört zu haben – wirkt sogar rückläufig: Unsere Generation wird immer ärmer, kränker, orientierungsloser und einsamer. In Ländern wie den USA sinkt inzwischen sogar die durchschnittliche Lebenserwartung (1). Wie ist das möglich bei all den technologischen Quantensprüngen der letzten Jahre (Digitalisierung, Automatisierung, Smartphone, Internet usw.)?

Der Grund dafür ist recht simpel, doch wird leider von unserer Gesellschaft sträflich missachtet: Es kommt darauf an, zu welchem ZWECK die Technologie eingesetzt wird! Die Autoren George Orwell und Aldous Huxley schilderten lebhaft ihre dunklen Visionen zwei verschiedener Wissenschaftsdiktaturen, in denen die Technologie nicht mehr dem Volk, sondern dem ZWECK der Herrschaft dient. Denn Technologie ist ein neutrales Mittel: So wie ein Messer gleichermassen zum Schneiden eines Brotes oder zur Ermordung eines unschuldigen Menschen eingesetzt werden kann, kann Technologie gleichermassen zur Befreiung oder zur Versklavung der Menschheit genutzt werden.

Das grosse Geheimnis, das Tech-Gurus wie Teslas Elon Musk oder Googles Eric Schmidt der Öffentlichkeit verschweigen, besteht darin, dass es etwas gibt, das über der Technologie steht und ohne das sich die Menschheit niemals von ihren Problemen befreien wird: Moralische Prinzipien, die immer Priorität haben müssen! Technologie und Wissenschaft werden nie in der Lage sein, unsere Zivilisation voranzubringen, wenn wir sie nicht den richtigen moralischen Werten unterordnen. Und das ist das grösste Problem der heutigen Zeit: Der technische Fortschritt kommt der breiten Bevölkerung nicht mehr zugute und fliesst nach oben die Hände einer kleinen technokratischen Herrscherklasse, die ihre digitalen Erfindungen nicht mehr in den Dienst der Moral, sondern von Herrschaft, Zwang und Gewalt stellt.

Heute dient die Technologie einer gegensätzlichen, bremsenden Kraft, die die menschliche Entwicklung zurückhält. Genau dem, was die Bibel mit dem Wort «Satan» beschreibt. Diese satanische Kraft, die sich an Gewalt und Zwang nährt, ist wie ein Virus, der uns befällt, versklavt und daran hindert, unser volles Potenzial zu entfalten.

Quelle: 1. faz.net, In Amerika sinkt die Lebenserwartung, 09.12.2016

Verlag	InfoXpress GmbH, Hohestr. 130, CH-4104 Oberwil
Kontakt	Tel +41 61 511 45 08 / info@expresszeitung.com
Website	www.ExpressZeitung.com
Erscheinung	10 x jährlich im Abonnement
Abo-Preis	Schweiz: SFr 69.- / EU: EUR 59.-
Bestellung	Tel +41 61 511 45 08 / abo@expresszeitung.com
Redaktion	Tilman Knechtel *(tk)* / Gerhard Wisnewski *(gw)* redaktion@expresszeitung.com
Gastautoren	Jeder Autor haftet für seine Aussagen selber.
Satz/Layout	Elementi Studio
Druck	DZZ Druckzentrum Zürich AG, CH-8021 Zürich
Logistik	Zehnder Druckerei, CH-9500 Wil
Fotos	Sofern nicht vermerkt: commons.wikimedia.org
Cover-Bild	Götz Wiedenroth, www.wiedenroth-karikatur.de
Nächste Ausgabe	April 2018

Jetzt abonnieren!

Nr. 4

Nr. 6

Nr. 7

Nr. 8

Nr. 9

Nr. 10

Nr. 11

Nr. 12

Nr. 13

Nr. 14

Das Abo kann auch rückwirkend ab Nr. 1 bestellt werden!

Online-Bestellung: www.ExpressZeitung.com
Jahresabo mit 10 Ausgaben:
Schweiz: SFr 69.- / EU: EUR 59.-

Thema der Ausgabe:

Das digitale Wohlfühl-Gefängnis

Wurden Menschen früher noch von ihren Nachbarn und Überwachungskameras bespitzelt, hat beim Thema Überwachung mittlerweile ein Paradigmenwechsel stattgefunden: Und zwar vom Zwang zur Freiwilligkeit, von der Nötigung zum Bedürfnis und von der Heimlichkeit zur Offenheit. Eine Überwachung, vor der sich jeder zu drücken versucht, wurde in eine Nachfrage verwandelt. Inzwischen steht der moderne Mensch Schlange für seine Wanzen: Ob das nun Smartphones, Computer oder elektronische Assistenten für zu Hause sind. Die flächendeckende Verwanzung der Erdbevölkerung mit mobilen Luxuswanzen vom Typ Iphone, Samsung Galaxy oder Amazon Echo würde kein Staat und keine internationale Organisation logistisch und finanziell hinbekommen, wenn die Verbraucher das nicht selbst besorgen würden.

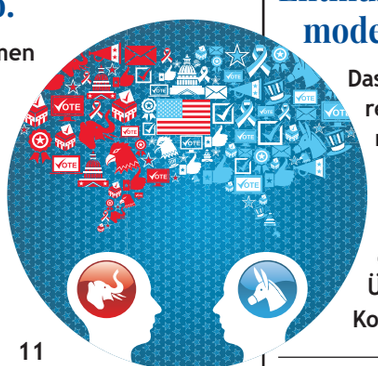
4

Technologie

Überwachung: Wenn Big Brother 1000 Augen und Ohren hat

Der moderne Mensch kauft sich seine Überwachungsgeräte selber und legt sich die Fesseln höchstpersönlich an. 4

Meinungskontrolle durch Google, Facebook, Amazon & Co.



Internetunternehmen wie Google, Facebook, Twitter, Amazon & Co. sind unermüdliche Datenlieferanten. Sie kennen die Vorlieben ihrer Nutzer oft besser als ihr Umfeld. 11

RFID-Technologie: Eine Zukunft ohne Geheimnisse?

RFID-Chips versetzen Datenschützer in helle Sorge: Sie könnten die Position eines jeden Menschen und dessen Interaktion mit Gegenständen rund um die Uhr durch eine grosse, verknüpfte Infrastruktur von Millionen Lesegeräten überwachen. 20

Politik

Angriff auf das Bargeld

Sollte das Bargeld eines Tages verschwinden, würde jeder einzelne Zahlungsvorgang überwachbar. Und da fast alles im Leben Geld kostet, wäre unser Leben ohne Bargeld künftig wie ein offenes Buch. 28

Technologie

Überwachung und Entmündigung durch moderne Autos

Das Auto der Zukunft soll dem Fahrer jegliche Eigenverantwortung nehmen und automatisch von einem Bordcomputer gesteuert werden. Doch das birgt grosse Gefahren: Wer nicht selbst steuert, unterwirft sich sowohl der Überwachung als auch der Kontrolle anderer. 32

Dauerüberwachung durch das digitale Stromnetz?

Die neuen digitalen Stromzähler könnten den Stromkonzernen oder der Regierung erlauben, jedes Gerät in Ihrem Haus nicht nur zu überwachen, sondern auch zu steuern. 42

Rauchmelder: Die Wanzen an der Zimmerdecke

Moderne Rauchmelder, deren Installation in deutschen Wohnungen inzwischen verpflichtend ist, haben das technische Potenzial, als Allzwecks-Überwachungsgerät zu dienen. 47

Smart Home, Smart City und das Internet der Dinge – Die Kontrolle über alles und jeden

Über das sogenannte «Internet der Dinge» sollen in Zukunft alle Gegenstände mit Chips, Sensoren, Datenspeichern oder Softwaresystemen ausgestattet werden, um sie über das Internet miteinander zu vernetzen. Theoretisch könnten auch Menschen, z.B. durch einen implantierten Chip, darin vernetzt werden. 50

Überwachung: Wer rennt, ist verdächtig - Resümée und Ausblick

Könnten wir bald in einem «Sozialen Kreditsystem» nach chinesischem Modell landen, in dem jeder, der sich systemkonform verhält, mehr Punkte bekommt und wer sich an den gerade aktuellen Vorgaben des Staates «versündigt» weniger Punkte? 57

Überwachung

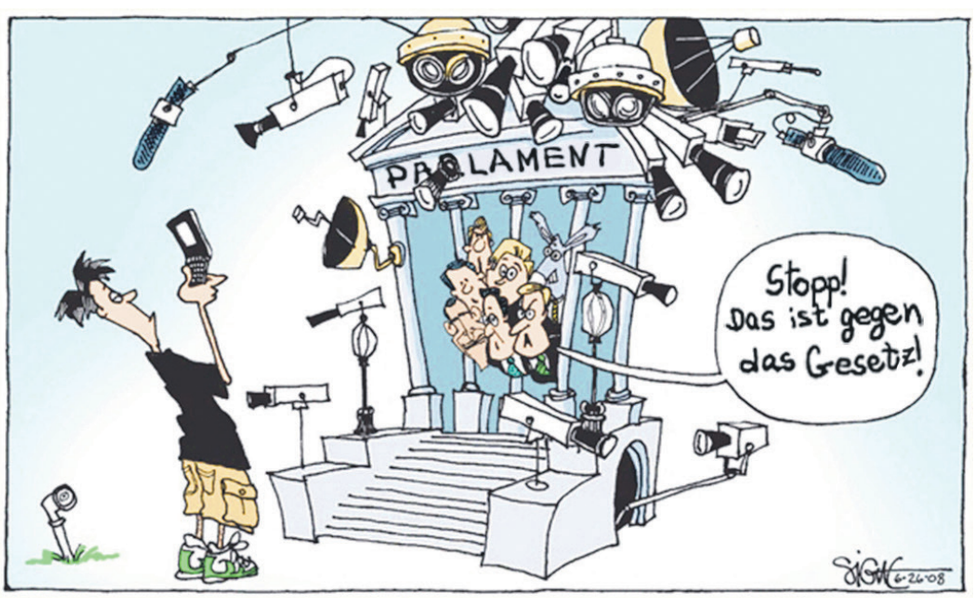
Foto: Shutterstock/Chesky

Überwachung:

Wenn Big Brother 1000

von Gerhard Wisnewski

Ein Mann in der Gewalt der Geheimdienste. Gruselig: von Satelliten bespitzelt, die Kreditkarten gesperrt, von oben bis unten verwanzt, der Ruf ruiniert, befindet er sich im Würgegriff der US-Schnüffelbehörde NSA. Er kann sich nicht bewegen, ohne fotografiert zu werden, er kann nicht telefonieren, ohne geortet zu werden, und er kann in kein Hotel einchecken, weil seine Kreditkarten nicht funktionieren. Kein Schritt, kein Atemzug und kein Gespräch bleiben verborgen. Zum Glück ist das nur Fiktion, nämlich aus dem Thriller «Der Staatsfeind Nr. 1». Aber was heisst «Fiktion»: Drehbuchautor David Marconi hatte die Überwachungstechniken der amerikanischen Überwachungsbehörde NSA schliesslich sorgfältig recherchiert. Und das zweite Problem: Das ist alles schon 20 Jahre her (1998). Und zwei Jahrzehnte sind bei der heutigen technischen Entwicklung eine Menge Zeit. Wirft man einen Blick auf den Alltag eines modernen Menschen, dann kann es ihm weitaus schlimmer ergehen als der Hauptperson in «Staatsfeind Nr. 1» – nur dass der moderne Mensch die elektronischen Fesseln vorerst nicht so spürt. Im Gegenteil, er kauft sich heute seine «Wanzen» selber und legt sich die Fesseln höchstpersönlich an.



Unsere Realität ist nicht mehr weit entfernt vom Orwell'schen Albtraum der Dauerüberwachung, in dem kein Schritt, kein Atemzug und kein Gespräch verborgen bleiben. Jedoch werden wir anders zur Preisgabe all unserer Handlungen, Aussagen und Geheimnisse gebracht, als sich George Orwell dies in seinem Roman 1984 vorgestellt hatte: Der moderne Mensch kauft sich seine Überwachungsgeräte selber und legt sich die Fesseln höchstpersönlich an.

«Herkömmliche» Überwachungsmethoden wie Kameras oder Spionagesatelliten werden zwar immer noch angewandt, doch können sie inzwischen längst nicht mehr mit der «Effizienz» digitaler Spionage mithalten: Durch Handys, Suchmaschinen, soziale Netzwerke, RFID-Chips, moderne Autos uvm. kann nahezu rund um die Uhr registriert werden, was wir alles so treiben. Nimmt man all diese Geräte zusammen, ist die digitale Überwachung weitaus «besser» als das, was Kameras jemals leisten könnten.

Das Internet macht neben der Überwachung auch eine Steuerbarkeit von aussen möglich, die Orwells Zukunftsvision gleicht. Auf jede Maschine, die mit dem Datennetz verbunden ist, kann grundsätzlich auch zugegriffen werden, egal ob Computer, Handy oder Auto.

Richtig interessant wird es allerdings erst, wenn man die Daten der unterschiedlichen Geräte und Accounts verknüpft und auswertet. Der Einblick in das Privatleben und die Persönlichkeit des Betreffenden dürfte atemberaubend sein. Dass diese Datenberge früher oder später bei den Geheimdiensten landen, ist schon lange kein Geheimnis mehr. Behörden wie die NSA verfügen mittlerweile sogar über eigene Suchmaschinen, mit denen sie sich über das digitale Verhalten von Millionen – wenn nicht Milliarden – Menschen informieren können.

Wie in Orwells Roman wird in der digitalen Welt nicht nur vom «Grossen Bruder» (Grosskonzerne und Geheimdienste) geschnüffelt. Auch die politisch treuen Mitbürger werden zur Denunziation ihrer Mitmenschen eingespannt: Dies geschieht durch Melde-Funktionen, die von den grossen Internetportalen angeboten werden. Durch das digitale Anschwärzen können politisch unerwünschte Inhalte aus dem Internet entfernt werden, ähnlich der Nachbearbeitung kritischer Textstellen in alten Büchern durch Orwells «Wahrheitsministerium».

George Orwell sah in seinem Roman 1984 ein Fernsehgerät namens «Televisor» vorher, das sowohl in der Lage ist, den Benutzer in seiner Wohnung zu überwachen, als auch mit ihm durch eine Kamera und ein Mikrofon in Kontakt zu treten. Die subtilen Einflussmöglichkeiten durch das heutige Internet hätte sich allerdings selbst Orwell nicht erträumen können.

Augen und Ohren hat

Der perfekte Lauschangriff

Wanze und Datenlieferant kann prinzipiell alles sein, was aufzeichnet, aufnimmt, ortet und auch funkt: Suchmaschinen, soziale Netzwerke, PC, Handy, Fitnessuhr, Auto oder auch Rauchmelder und anderes mehr. Fitness-Gadgets erheben intimste Details über unseren Gesundheitszustand und unsere Leistungsfähigkeit, während praktische Helfer wie Amazon Echo (der u.a. auf den Namen «Alexa» hört), zu den besten Abhörgeräten zählen, die je gebaut wurden: Es verfügt nicht nur über Richtstrahltechnologie und Geräuschunterdrückung, sondern auch über nicht weniger als sieben Mikrophone. Damit «hört Echo Sie aus jeder Richtung – sogar wenn Musik läuft», verspricht Amazon. Denn das ist schliesslich nicht schlimm, sondern praktisch, glaubt der moderne Mensch. Und funktionieren tut es auch: «Die eigentliche Spracherkennung der eigenen Stimme funktioniert bei Alexa im Test erstaunlich gut», lobte die Computerzeitschrift Chip: «Selbst aus grösserer Entfernung und bei Umgebungsgeräuschen wie lauter Musik versteht die freundliche und natürlich klingende Computer-Assistentin jedes Wort.» [1].

Amazon Echo tätigt Anrufe, spielt Musik ab, stellt Wecker und Timer, führt den Kalender, informiert über das Wetter, die Verkehrslage und Sportergebnisse, verwaltet Einkaufslisten und anderes mehr. Von kleinen Verständigungsproblemen abgesehen. Kurz: Der US-Multi Amazon will unser gesamtes Leben managen und wird so zu einem Familienmitglied, das wahrscheinlich mehr mitbekommt als jeder andere. Ganz einfach, weil seine Ohren immer offen sind. **Denn sowohl Amazon Echo als auch sein Pendant Google Home hören ständig mit – Tag und Nacht. Denn sonst könnten sie ja nicht reagieren. So überwachen sie unseren Alltag und unseren Privatbereich komplett – sogar ob sich plötzlich weitere Personen im Haushalt aufhalten, können sie im Prinzip mitbekommen, und zwar mittels Stimmerkennung. Zwar sind sie angeblich immer nur auf der Suche nach Vorlieben, Bedürfnissen und Wünschen. Aber diese Vorlieben, Bedürfnisse und Wünsche landen zusammen mit weiteren Daten eben sehr wahrscheinlich irgendwann bei den Geheimdiensten - ob mit oder ohne Zutun des jeweiligen Unternehmens.**

Smart ist nur der Schnüffler

Neben den aufmerksamen Mikrophonen und Lautsprechern gibt es noch eine wachsende Zahl von weiteren Geräten, die

lauschen, sehen und registrieren sollen, was wir den Tag über so alles treiben. Man nennt sie «Internet der Dinge» oder auch «Smart Home». Smart ist daran gar nichts, ausser den Entwicklern und Verkäufern, die uns diese Geräte andrehen, als da wären «smarte» Überwachungskameras, Rauchmelder, Herde, Waschmaschinen, Kühlschränke, Rollläden, Heizungen und Kaffeemaschinen: **Alles soll mit dem Internet verbunden werden und so jederzeit von aussen steuerbar sein – von wem auch immer. Denn jede Maschine, die mit dem Datennetz verbunden ist, kann grundsätzlich auch gehackt werden, ob nun von privaten Eindringlingen oder vom Staat. Und jedes dieser Geräte wirft Daten ab: Wann und wie Sie Ihre Wäsche waschen, wann Sie aufstehen und zu Bett gehen (Wecker, Kaffeemaschine, Rollläden), wann und was Sie fernsehen, und, und, und. Schon jetzt sind Millionen Mieter und Hausbesitzer online, ohne dass ihnen das bewusst ist, nämlich durch drahtlose Heizungszähler, Wasseruhren und Rauchmelder. Drahtlose Stromzähler, die jede Veränderung des Stromverbrauchs protokollieren, werden bald folgen (siehe S. 42). Nimmt man all diese Geräte zusammen, ist das fast noch «besser» als eine Kamera. Und zwar deshalb, weil das Smart Home in der Lage ist, so etwas wie einen Fingerabdruck von uns zu generieren, nämlich ein Lebensprofil.**

Immer auf dem Radarschirm

Hat man weder Echo noch Google Home zu Hause, ist das für potenzielle Schnüffler auch nicht schlimm - denn schliesslich gibt es ja noch Handy und PC, ausgestattet mit Mikrophon und Kamera. Beides kann man sehr einfach von aussen steuern und abhören, wobei zum Beispiel Programme vom Typ «Keylogger» («Tastaturrekorder») auch die Tastatureingaben protokollieren. Wer erst einmal Zugriff auf den Rechner und seine Festplatte hat, kann den gesamten Datenbestand durchforsten. Und verlässt man mal die Wohnung, ist das auch kein Problem, denn draussen warten bereits Millionen Überwachungskameras in Geschäften und auf öffentlichen Plätzen. Ausgerechnet die «Orwell-Stadt» London (wo der grösste Teil des Romans «1984» spielt) ist die Kamera-Hauptstadt Europas, vielleicht sogar der Welt: «Wer hier lebt, der weiss, dass er an fast jeder Ecke von einer Kamera gefilmt wird - gleich, ob im Kaufhaus oder im Supermarkt, in der U-Bahn oder auf öffentlichen Strassen und Plätzen. Auch in vielen Siedlungen mit Sozialwohnungen, etwa im Stadtteil Hackney, ist die Videoüberwachung grossflächig angelegt, sagt einer der Bewohner: ‚Die Kameras sind überall, sie zeigen in alle Richtungen'», berichtete der Deutschlandfunk (online,

Seite 5

23.12.2016). Fieberhaft arbeiten Softwareingenieure in aller Welt auch an einer Gesichtserkennung, die Straftäter automatisch erkennen soll. Das Problem dabei ist nicht die Fähigkeit an sich, sondern ob die Technologie eines Tages in die Hände eines Erdogan oder eines anderen «Grossen Bruders» gelangt. Die gute Nachricht: Manche Städte lassen die Kameras inzwischen wieder abbauen.

Superwanze Handy

Aber auch wenn wir nicht in das Visier einer Kamera geraten: Unsere Wanze haben wir ja immer dabei - das Smartphone, die zarteste Versuchung, seit es Wanzen gibt. Es ist nicht nur ein vollwertiger Computer und verfügt nicht nur über Mikrophone und Videokameras, sondern auch über einen GPS-Empfänger und Bewegungssensoren. Über die Mobilfunkverbindung und erst recht den GPS-Sensor kann es genau geortet werden. Manche legen es nachts auch neben das Bett. Gespräche oder Geräusche können aufgezeichnet, Fotos, Videos, SMS und andere Dateien bei Bedarf heruntergeladen werden. Und zwar nicht nur von den sogenannten «Sicherheitsbehörden», sondern von jedermann! Für das Ausspionieren von Handys gibt es öffentlich zugängliche Portale, wie zum Beispiel mSpy. Offiziell handelt es sich um ein Überwachungssystem für Eltern von minderjährigen Kindern – dem abgehörten Smartphone oder PC ist es aber egal, ob sein Besitzer volljährig ist oder nicht. Genausogut kann es sich bei dem Lausch- und Spähopfer um die Ehefrau, Freundin oder den Angestellten einer Firma handeln: «Unsere Mobile-Monitoring-Software arbeitet auf dem Ziel-Gerät und protokolliert dessen sämtliche Aktivitäten, inklusive Anruf-Protokolle, GPS-Position, Kalender-Updates, Text-Mitteilungen, E-Mails, Surf-Verhalten und vielem mehr! Haben Sie mit Hilfe unserer unkomplizierten Schritt-für-Schritt-Anleitung Ihr persönliches mSpy-Online-Nutzerkonto erstellt, können Sie sich sofort einloggen und die erfassten Daten abrufen.» Vom Normalbürger zum NSA-Agenten in zehn Minuten, sozusagen. Der Spitzel braucht nur für ein paar Minuten Zugriff auf das auszuspähende Telefon, und schon kann es losgehen. Zwar muss man das Spähopfer informieren – aber ob sich der Schnüffler daran hält, steht auf einem anderen Blatt. So kann man die Anruflisten des «Smartphones» durchblättern (samt Dauer und Uhrzeit), bestimmte Rufnummern sperren, Instant-Messages, SMS-Nachrichten und E-Mails lesen, GPS-Position und Internetverhalten aufzeichnen, im Kalender und Adressbuch schmökern, Apps sperren oder freigeben, Fotos, Videos und Musik sichten und bei Bedarf auch downloaden.

Jeder kann Agent werden

Natürlich kann man auch das Mikrophon einschalten und die Aufnahmen als mp3-Datei mitschneiden. Darüber hinaus erstellt die Software Auswertungen über die gesamte Handy-Nutzung, also was wann auf dem Gerät stattgefunden hat und wie lange (=komplettes Nutzerprofil). Etwas Ähnliches gibt's selbstverständlich auch für den PC und Mac: einschliesslich Bildschirmfotos, Keylogger und Informationen über die Nutzeraktivitäten, die Programmnutzung und die installierten Anwendungen.

Kurz: Das Spähequpiment für den Amateur-Agenten steht dem der Profis auf vielen Feldern in nur wenig nach, angefangen bei mit Kameras gespickten «James-Bond-Utensilien» wie Brillen, Uhren, Weckern oder Rauchmeldern bis hin zu fliegenden Drohnen, die mal einen Blick in Nachbars Garten werfen: «Datenschützer befürchten massive Späh-Angriffe auf die Privatsphäre der Bürger. Dabei ist der Angreifer diesmal kein internationaler Multikonzern, sondern womöglich der eigene Nachbar», schrieb die Welt schon 2012. «Denn Überwachungstechnik, die früher Militär und Polizei vorbehalten war, gibt's nun günstig für den neugierigen Otto Normalverbraucher: Er schickt eine mit HD-Kameras ausgerüstete Drohne zum Spionageflug ins Privatleben seiner Opfer» [2].

Schlüsselloch Nr. 12

Apropos Fliegen: Was ist eigentlich mit den Spionagesatelliten, die in «Staatsfeind Nr. 1» dem Spähopfer auf den Fersen waren? Nun, da sind wir natürlich auch wieder bei Google, nämlich bei Google Earth und Google Maps. Ein Teil der dort zur Verfügung gestellten Bilder stammt von Satelliten, die hochauflösenden Aufnahmen eher von Flugzeugen. Da diese Bilder Monate bis Jahre alt sind, eignen sie sich zwar nicht für eine zeitnahe oder gar Echtzeitüberwachung. Aber immerhin arbeitet dieses Luftbild-Portal in Ballungsgebieten und Städten mit einer Auflösung von fünfzehn bis zu fünf Zentimetern, so dass man sich beispielsweise ein wenig über die Wohnverhältnisse anderer Menschen informieren kann. Und mit der Ausforschung der Wohnung fängt Bespitzelung ja schliesslich an. So können beispielsweise auch Einbrecher besser Ein- und Ausgänge sowie Fluchtwege auskundschaften, Nachbarn, Behörden und andere Interessierte sich über den Lebensstil (Swimming Pool?) oder den einen oder anderen Schwarzbau informieren. Was die militärischen Spionagesatelliten können, ist naturgemäss zwar Gegenstand von Spekulationen. Aber gewisse physikalische Grenzen gibt es schon. So zeigen Berechnungen, dass auch ein moderner Spähtrabant wie «Keyhole 12» («Schlüsselloch 12») mit seinem Vier-Meter-Teleskop kaum über Auflösungen von fünf Zentimetern hinaus kommen dürfte, so dass sich Gesichter oder Nummernschilder nur schlecht identifizieren liessen. Für die Erkennung von Militärfahrzeugen, Truppenbewegungen, Abschussrampen und Kriegsschäden reicht es aber allemal, genauso wie für Ernten und Unwetterschäden. Der Hauptvorteil liegt in der Aktualität: Indem die Satelliten ihre Bilder praktisch in Echtzeit zu den Bodenstationen übertragen, ist man über das jeweilige Spähobjekt zeitnah informiert.

Die legale Spionage-Software mspy muss nur auf dem Smartphone eines anderen installiert werden und schon kann der Nutzer von mspy über sein Smartphone jede Smartphone-Aktivität inklusive Position des Überwachten nachverfolgen. Dass Telekommunikationsanbieter und Geheimdienste dies ebenfalls können, liegt auf der Hand.

Von der Überwachung zur Steuerung

Nummernschilder kann man, wie gesagt, wahrscheinlich (noch) nicht deutlich aus dem All erkennen – muss man aber auch gar nicht. Für Autos gibt es ja noch die Kennzeichenleser an den Autobahnen – nur vernetzt müssen die Daten noch werden. Ausserdem werden Kraftfahrzeuge ja auch anders geortet, etwa über ihre bordeigenen GPS-Geräte, wie beispielsweise Bordtelefone. Ist das Auto «getagged»,

Aufnahmen der Spionage-Satelliten ergänzen die digitale Datenflut.

also mit einer GPS-Wanze versehen, erkennt es der Satellit auch ohne Nummernschild. Sind die Insassen mit Mobilfunk unterwegs, kann man sie ohnehin unabhängig vom Verkehrsmittel orten – und gegebenenfalls von einer Drohne aus töten. Die Handys funktionieren dabei als elektronische Zielmarkierungen, die direkt von dem jeweiligen Geschoss angesteuert werden. Vielleicht kann man das Fahrzeug ja auch von einem Spionageflugzeug aus erkennen, beispielsweise einem modernen Nachfolger der legendären U-2, die in den sechziger Jahren Kuba und die Sowjetunion bespitzelte. Schon jetzt konstruieren Internetkonzerne auch Solardrohnen wie die Solara 50, die jahrelang in grosser Höhe über einem bestimmten Fleck kreisen soll. Je nach Nutzlast sind diese Drohnen zu allem fähig: Zur Versorgung eines Gebietes mit Mobilfunk oder Internet genauso wie zur «Aufklärung».

Je mehr Elektronik an Bord eines fahrbaren Untersatzes ist, umso besser ist es jedenfalls für Behörden und andere Schnüffler: «Ohne Elektronik funktioniert in einem modernen Auto fast nichts mehr. Die Computer und Steuergeräte im Wagen sammeln Daten, die viel über das Auto aussagen – aber auch über den Fahrer», meinte die Welt: «Die Rechner können Informationen wie Geschwindigkeit, Bremsleistung und Beschleunigung speichern. [...] Mit den Daten lassen sich auch Rückschlüsse auf das Fahrverhalten ziehen. Nach einem Unfall sind das interessante Informationen für Polizei und Versicherungen. [...] Assistenzsysteme können problemlos ein Fahrerprofil erstellen» [3]. «Cyberattacken und Hackerangriffe auf Autos» seien «keine Zukunftsvisionen mehr», meinte 2017 die Website Trojaner-Info (18.1.2017). Die Überwachung von Auto-Bordcomputern und Standorten sei «wohl schon seit 15 Jahren» möglich. In den letzten Jahren seien «bereits VW-Autos gehackt» worden, «vor kurzem erst wurde Tesla von Hackern unter Kontrolle gebracht» (gemeint ist wohl ein Tesla-Fahrzeug). Sowohl Forbes.com als auch golem.de hätten berichtet, dass es gar keiner neueren GPS-Systeme bedürfe, «um Fahrer zu orten, auszuhorchen sowie Profile bzw. Metadaten zu sammeln, zu speichern und auszuwerten. **Es wird kolportiert, dass mit den integrierten Sensoren und den integrierten Bordsystemen seit rund 15 Jahren Autos digital verwanzt werden.» Wobei der Trend von der passiven Überwachung in Richtung aktiver Eingriffe in das Fahrgeschehen geht. Stichwort: «Selbstfahrendes Auto».** Dann fahren nicht mehr wir, sondern entweder der Computer oder Big Brother – oder beide zusammen. Wie die deutsche Bundeskanzlerin Angela Merkel im Juni 2017 vor argentinischen Studenten erklärte, werde man in 20 Jahren nur noch mit einer Sondergenehmigung selbst ein Auto steuern dürfen [4] (siehe S. 40).

Chip im Arm

Zeitgenossen, die sich für besonders progressiv halten, lassen sich (wie einem Haus- oder Nutztier) sogar einen sogenannten RFID-Chip (Radio Frequency Identification) mit persönlichen Daten unter die Haut implantieren, der berührungslos von geeigneten Scannern ausgelesen werden kann (siehe S. 20). Auch das funktioniert ganz freiwillig, etwa, wenn sich Diskobesucher ihre «Eintrittskarte» unter die Haut «spritzen» lassen. Der spanische Baja Beach Club sei weltweit die erste Diskothek gewesen, die 2004 mit dem implantierten Chip Schlagzeilen gemacht habe, berichtete das Computerportal heise.de: «Mit einer Party im März 2004 feiert die Szene-Discothek ‚Baja Beach' in Barcelona ihren siebten Geburtstag. An diesem Abend will der Club mehr bieten als nur Spass bei Strandatmosphäre. Erstmals können sich gut betuchte Stammgäste gegen Geld einen reiskorngrossen Chip in den Arm spritzen lassen, der die Funktion der Geldkarte übernimmt: Indem sie sich an einem Lesegerät vorbeibewegen, können sie damit künftig ihre Zeche begleichen.» Danach sei die Idee durch Europa getourt: «Die ‚Bar Soba' in Glasgow bietet den Gästen die Chipspritze an und auch der niederländische Ableger des Baja Beach Club in Rotterdam» (22.10.2009). Da bei manchen Tieren rund um den RFID-Chip dummerweise Krebsgeschwüre entstanden, kam die Technik wieder in Verruf.

Rosa Elefant im Wohnzimmer

Die Grenzen zwischen Software, Spyware und Malware sind fliessend. Ist zum Beispiel Google nun eine Suchmaschine oder eine Spyware? Erfährt der Konzern nicht mehr über uns als wir über unsere Suchobjekte? **Während viele in Sachen Überwachung über die Fliege an der Wand diskutieren, sieht kaum jemand den rosa Elefanten im Wohnzimmer: nämlich die grössten Spyware-Portale überhaupt wie Google, Facebook, Twitter, und wie sie alle heissen. Bei ihnen allen fallen Hunderte bis Tausende von Seiten dicke Dossiers über uns an, die nur darauf warten, mit anderen Dossiers zu einer riesigen elektronischen Akte verschmolzen zu werden.** (siehe S. 11) Auf den Antrag des Österreichers Max Schrems hin schickte ihm zum Beispiel Facebook 2011 sein ganz persönliches Dossier zu: Alle Aktivitäten, die Schrems jemals in dem «sozialen Netzwerk» unternommen hatte. Auf einer CD erhielt er eine PDF-Datei mit nicht weniger als 1222 Seiten, darunter auch Inhalte, die er längst gelöscht zu haben glaubte.

«How the CIA made Google»

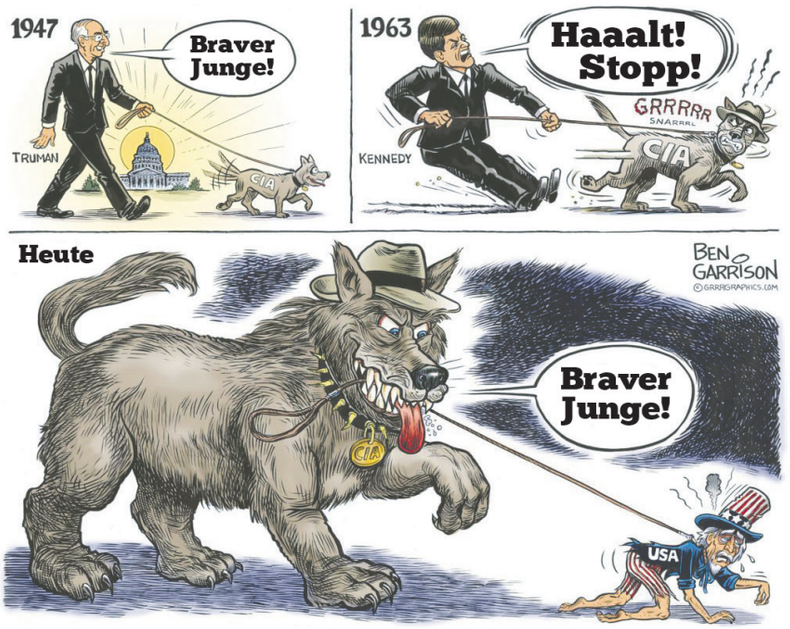
Das naheliegendste Motiv ist zwar Profit: Mit ihrer Datensammelwut bekommen die Konzerne Milliarden von wertvollen Profilen der Verbraucher, denen sie dann wieder massgeschneiderte Werbung einblenden können. «Wie weit das gehen kann, demonstriert zum Beispiel Amazon», hiess es auf der Web-

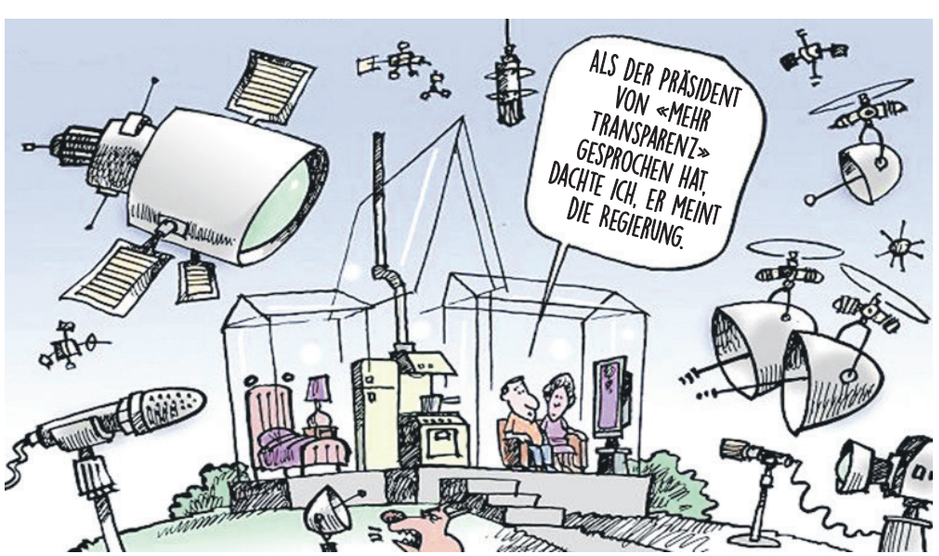
Seite 7

site billiger-telefonieren.de: «Da alle auf dem Markt etablierten Methoden des maschinellen Lernens nicht ausreichten, baute der Internetriese einfach ein eigenes System, das gewaltige Datenmengen verarbeiten kann, aber trotzdem schon nach wenigen Klicks weiss, was Sie als nächstes kaufen. [...] Eine der Zukunftsvisionen, die man bei Amazon entwickelt hat, ist, Lieferungen auf den Weg zu schicken, bevor der Kunde überhaupt weiss, dass er etwas kaufen will» (10.1.2017). Gewinn ist aber nicht das einzige Motiv. Die CIA zum Beispiel mauserte sich über ihre eigene Investmentfirma In-Q-Tel klammheimlich zu einer Art Holding für lauter kleine und grössere Daten-Unternehmen. Dazu sollen angeblich auch Google und Facebook gehören – zwei Konzerne, die praktisch alles über uns wissen, insbesondere über diejenigen, die dort treudoof ihr Privatleben eintippen: «Wie die CIA Google machte» lautete eine Überschrift auf der Nachrichten-Website medium.com. Demnach habe man «einige vielversprechende Studenten» unterstützt: «Einer von ihnen war Sergey Brin, der Gründer von Google» (5) (siehe S. 16).

Ein Dossier mit 1222 Seiten

Richtig interessant wird es erst, «wenn man die Daten verknüpft», also auswertet, meint Facebook-Kritiker Schrems. Diese Auswertungen müsse Facebook «aber nicht herausgeben». Dabei wird es da ja erst richtig spannend: Der Einblick in das Privatleben und die Persönlichkeit des Betreffenden dürfte atemberaubend sein. Noch spannender wird es, wenn die Daten aller sozialen Netzwerke, Suchmaschinen, Banken, Kreditkartenunternehmen und Versandhändler zu einer riesigen Akte zusammengeführt werden. Während EU-Bestimmungen die Weitergabe der Daten an Geheimdienste verböten, verpflichteten US-Gesetze Facebook sogar «dazu, der NSA bei der Massenüberwachung zu helfen». Da haben wir den Salat. Sind die «sozialen Netzwerke» also wirklich nichts weiter als Spyware-Portale? Denn drei Mal dürfen Sie raten, an welche Gesetze sich die US-Internetriesen wohl halten werden: an die der EU oder an jene der USA? **Aufgrund des Foreign Intelligence Surveillance Act (FISA) seien Daten von Nicht-US-Bürgern nicht vor dem Zugriff US-amerikanischer Geheimdienste wie der NSA geschützt, hiess es auf netzpolitik.org (4.10.2017). Demnach können die Datenberge der einzelnen sozialen Netzwerke also tatsächlich bei den Geheimdiensten landen. Mit anderen Worten kann irgendwo in Langley (CIA) oder in Fort Meade (NSA) ein Beamter Ihren Namen eingeben und erhält daraufhin sowohl Ihre Rohdaten (die Sie selbst eingegeben haben), Ihre Metadaten (die sich aus den Rohdaten ergeben) als auch jede erdenkliche Auswertung.** Ja, man darf sogar fragen, ob das nicht letztlich der eigentliche Sinn dieser «asozialen Netzwerke» ist.





Atemberaubende Einblicke

Papperlapapp: Das kann doch nicht sein! Das kann schon sein. 2013 flog zum Beispiel die Schnüffelsoftware XKeyscore auf. Schon vergessen? «Dokumenten des Whistleblowers Edward Snowden zufolge erlaubt ein hoch geheimes Programm der National Security Agency, Analysten ohne Autorisierung riesige Datenbanken aus E-Mails, Online Chats und Browser-Verläufen von Millionen Menschen zu durchsuchen», schrieb damals der britische Guardian (online, 2.8.2013). Im Vergleich zu diesen Super-Suchmaschinen ist Google nur ein Zulieferer – ob absichtlich oder unabsichtlich. Neben XKeyscore gibt es noch weitere geheimdienstliche Suchwerkzeuge: Die NSA zum Beispiel «stellt 23 Sicherheitsbehörden in den USA eine geheime, interne Suchmaschine zur Verfügung», hiess es ebenfalls auf netzpolitik.org: «Sie soll über 850 Milliarden (genau: 850.000.000.000) Einträge systematisch durchsuchen können.» Die NSA-Suchmaschine trage den Namen ICREACH und «soll angeblich über eine ähnliche Suchmaske wie Google verfügen.» Angeblich haben «über 1000 Analysten aus 23 US-Regierungsbehörden Zugang zu ICREACH», heisst es auf der geheimdienstkritsichen Nachrichtenseite The Intercept: «Über ICREACH geteilte Informationen können dazu verwendet werden, Bewegungsprofile und persönliche Netzwerke zu erkennen, zukünftige Handlungen vorherzusagen und potenziell auch religiöse und politische Ansichten aufzudecken» (6). «Die NSA-Suchmaschine soll in der Lage sein, 2 bis 5 Milliarden neue Daten täglich zu verarbeiten, darunter 30 verschiedene Arten an Metadaten über Emails, Telefonanrufe, Faxsendungen, Internetchats, Textnachrichten und Standortdaten von Handys.» Und natürlich kann man auch diese Super-Suchmaschinen in «Meta-Suchmaschinen» zusammenfassen, also in übergeordnete Suchmaschinen, die

alle irgendwo gespeicherten Datenbestände zusammenführen und durchforsten. Diese Datenberge listen nicht nur einfach endlose Datenkolonnen und Fakten auf, also welche Bücher wir bestellt, welche Internetseiten wir angeschaut, welche E-Mails wir geschrieben und welche Einkäufe wir getätigt haben. Sondern die Programme durchdringen und analysieren unsere Persönlichkeiten auch immer gründlicher und tiefer.

Wolf oder Wanze

Wobei wir bei all der Technik eins nicht vergessen dürfen: Eine der wichtigsten Wanzen ist immer noch der Mensch, im Geheimdienstjargon kurz «HUMINT» genannt – menschliche Quelle. Der klassische lateinische Spruch «homo homini lupus est» («Der Mensch ist des Menschen Wolf») ist veraltet. Heute muss es heissen: «homo homini cimex est» – der Mensch ist des Menschen Wanze.

Wie schon im Kommunismus und Nationalsozialismus gehören Verdächtigungen, Denunziation und Repressalien wieder zusammen. 73 Jahre nach dem Ende des Dritten Reiches und 27 Jahre nach dem Ende der Sowjetunion ist Anschwärzen wieder schick. Internetportale bauen überall Melde-Funktionen ein, politische Parteien und Gruppen rufen ihre Mitglieder zur Denunziation auf. Staatsfeind Nr. 1 ist der Internetnutzer, der allzu unverblümt seine Meinung äussert. Über die Bekämpfung rechtswidriger Inhalte geht das weit hinaus. «Wir sprechen uns gegen Hate Speech aus, egal ob strafbar oder nicht», heisst es beispielsweise in einem verräterischen Statement des deutschen Bundesinnenministeriums, das seine Kompetenzen damit deutlich überschreitet. Denn jenseits der Strafbarkeit oder Rechtswidrigkeit hört die Zuständigkeit des Staates für Meinungen und Stilfragen auf.

Staatsfeind Nachbar

Staatsfeind Nr. 2 ist natürlich der Nachbar: «Wenn wir in der Nachbarschaft irgendetwas wahrnehmen, dass da plötzlich drei etwas seltsam aussehende Menschen eingezogen sind, die sich nie blicken lassen oder ähnlich, und die nur Arabisch oder eine Fremdsprache sprechen, die wir nicht verstehen, dann sollte man glaube ich schon mal gucken, dass man die Behörden unterrichtet, was da los ist», meinte zum Beispiel Berlins Innensenator Ehrhart Körting (7). Nach dem Motto: «Kein Geheimdienst der Welt kriegt so viel spitz, wie ein Weib, das in der Nachbarschaft sitzt», wie der russiche Poet Démjan Bedny dichtete. Die in Deutschland berüchtigte Amadeu Antonio Stiftung (die sich angeblich für Menschenrechte, Toleranz und gegen Rassismus einsetzt) rufe sogar dazu auf, «nicht justiziable Aussagen in sozialen Netzwerken

Werden mit Googles «Perspective» bald kritische Kommentare entfernt?

Mit seinem neuen Service «Perspective» bietet Google eine (bisher noch freiwillige) Möglichkeit, mit der insbesondere Nachrichtenwebseiten Kommentare von Lesern auf ihre «Giftigkeit» prüfen können. Macht man die Probe aufs Exempel, kommt dabei aber eine eher ganz neue Form von Zensur und Gedankenkontrolle heraus, ganz im Sinne des «Weltverbesserers» Google und seiner an diesem Experiment beteiligten Partner Wikipedia, The New York Times, The Economist und The Guardian.

Google versteht unter «giftigen Kommentaren» Aussagen, die Diskussionen stören und andere Nutzer beleidigen oder mobben. Das Programm liefert mit Hilfe künstlicher Intelligenz für einen übermittelten Kommentar den Punktwert der «Giftigkeit». Neue Kommentare werden mit Mustern in der Datenbank verglichen, dann wird ein Artikelwert zwischen 0 und 100 ermittelt. Je höher der Wert, desto «toxischer» ist ein Kommentar und demnach auch umso geeigneter zur Löschung. «Die Software lernt ständig dazu», sagt Jared Cohen, Chef der Entwicklerfirma Jigsaw.

Auf der Webseite von Perspective kann jeder den neuen Service, der im Moment nur auf Englisch angeboten wird, selber testen. Die Webseite Jouwatch hat das getan und ihr Ergebnis fällt eindeutig aus: Diese Software ist der Versuch, die Meinungsfreiheit in politisch korrekte Bahnen zu lenken. Sie ist daher ein gefährliches Werkzeug in den Händen der Meinungsmacher und der marxistischen Ideologen, die in den Krieg der Worte gezogen sind, um ihren politischen Gegnern den Mund zu verbieten.

Hier einige Beispiele:

10% likely to be perceived as 'toxic'

i don't like christians

66% likely to be perceived as 'toxic'

i don't like muslims

Der Satz «Ich mag Christen nicht» ist nur 10% giftig, der Satz «Ich mag Muslime nicht» allerdings 66%. Hier wird der Islam eindeutig «bevorzugt». So viel zum Thema Gleichheit der Religionen.

87% likely to be perceived as 'toxic'

kill the infidels wherever you find them

87% likely to be perceived as 'toxic'

thou shalt not kill

Die erste Anfrage behandelt die Koran-Sure 2, Vers 191 – «Und tötet sie, wo immer ihr auf sie trefft». Die zweite Anfrage stammt aus dem Buch Moses und ist das 5. Gebot «Du sollst nicht töten». Eine Kriegserklärung aus dem Koran wird demnach als gleich toxisch angesehen wie das christliche Gebot der Nächstenliebe.

84% likely to be perceived as 'toxic'

i don't like black people

63% likely to be perceived as 'toxic'

I don't like white people

«Ich mag schwarze Menschen nicht» ist 84% giftig, «Ich mag weisse Menschen nicht» nur 63%. Das ist eindeutig Rassismus vom Feinsten!

5% likely to be perceived as 'toxic'

i don't like heterosexual people

66% likely to be perceived as 'toxic'

i don't like gay people

Der Satz «Ich mag heterosexuelle Menschen nicht» ist nur 5% giftig, dagegen ist der Satz «Ich mag schwule Menschen nicht» 66% giftig. Eigentlich müsste man gerade bei diesem Thema davon ausgehen, dass die sexuelle Orientierung keine Rolle spielt. Das Gegenteil ist der Fall. Schwule nicht zu mögen ist «toxischer» als etwas gegen Heterosexuelle zu haben.

Theoretisch könnte es bald dazu kommen, dass Google Kommentare ab einer gewissen Giftigkeit automatisch löscht. Schon jetzt ist klar zu erkennen, dass sich die Suchmaschine den Dogmen der heutigen Politik angepasst hat, höchstwahrscheinlich weil sie in Wahrheit ein Produkt dieser Politik ist.

Quelle: journalistenwatch.com, Wie Google unser Denken «vergiften» will!, 30.07.2017

Die mit dem Verfassungsschutz zusammenarbeitende Amadeu Antonio Stiftung veröffentlichte einen «Crashkurs», der erläuterte, wie man mit der Melde-Funktion sozialer Netzwerke zum Online-Denunzianten politisch unkorrekter Nutzer werden kann.

Seite 9

zu melden und zur Anzeige zu bringen», monierte Dorothee Dienstbühl, Professorin an der Fachhochschule für öffentliche Verwaltung in Nordrhein-Westfalen. Es stelle sich «die Frage, womit die Löschung von Inhalten und die Sperrung von Nutzerprofilen gerechtfertigt sind, wenn sie keine Straftat darstellen und nicht die Rechte anderer verletzen. Denn diese Praxis steht, wie es scheint, dem hohen und grundgesetzlich verbürgten Gut der Meinungsfreiheit (Art. 5 GG) entgegen.»

Gerade die Leiterin der Amadeu Antonio Stiftung, Anetta Kahane, sei umstritten: Als «IM Victoria» habe sie in der DDR «von 1974 bis 1982 für die DDR-Staatssicherheit Privatpersonen ausspioniert». Die IM-Akte «Victoria» habe fast 800 Seiten umfasst, von denen nur die Hälfte freigegeben worden sei (8). Heute arbeitet Kahane nicht nur mit dem Verfassungsschutz zusammen, sondern in der Leitung der Amadeu Antonio-Stiftung sitzt neben Kahane sogar der Präsident des Thüringischen Verfassungsschutzes, Stephan Kramer –womit sie sich endgültig als Schnüffel- und Propagandastiftung entlarvt. Unter der Überschrift «Onlinehetze» gibt die Stiftung einen Crashkurs in Sachen Denunziation bei Facebook, YouTube und in anderen «sozialen Netzwerken»: «Alle Netzwerke bieten die Möglichkeit, einen Beitrag zu melden an. Meistens befinden sich die Buttons zum Melden, in dem zu meldenden Post selbst. Manchmal müssen noch ein, zwei Klicks gemacht werden.» – «Augen offen halten, bespitzeln, melden» – damit sind wir schon sehr nahe an den vor allem kommunistischen Überwachungsmethoden eines Stalin oder eines Erich Honecker (die ansonsten nicht zu vergleichen sind). Und auch die Nationalsozialisten waren schliesslich «Parteigenossen», sprich: Sozialisten. Und wenn man sich den heutigen Gesinnungsterror und die Jagd auf «Meinungstäter» einmal anschaut, dann werden all die eifrigen Jäger vor lauter Nazi-Jagd dabei noch selber zu Nazis.

Anonyme Briefe gibt's nicht mehr...

Wenn Sie jetzt etwa ungehalten über all diese Schnüffelei sein sollten und einmal einen geharnischten Brief an die Regierung oder an einen der erwähnten Internetriesen schreiben wollen: Tun Sie das. Aber bitte nicht anonym. Denn anonyme Briefe gibt es praktisch nicht mehr: «Digitale Kopierer hinterlassen auf den Ausdrucken Signaturen, über die das genutzte Gerät identifiziert werden kann (der ‚Machine Identification Code', beim BKA als ‚Farbdruckermarkierung' oder ‚Tracking Dots' bekannt)» (9). Auch wenn man einmal finanziell klamm ist, sollte man nicht auf den Kopierer zurückgreifen, denn viele Kopierer seien in der Lage, «das Kopieren von Banknoten oder Wertpapieren selbst zu erkennen (‚Banknotenerkennungssysteme').» Manche Geräte holen auch gleich die Polizei: «Teilweise verfügen die Kopierer über eine Verbindung zum Internet und können bei einer Behörde einen Alarm ausgeben. Inwiefern dies praktiziert wird, bleibt aber offen».

Datenseen austrocknen

Aber mal ehrlich: Niemand von uns will mehr in die Zeit vor dem Internet zurück – und vielleicht auch nicht in die Zeit vor dem Mobiltelefon. Genauso wenig wie in die Zeit vor der Einführung der Elektrizität. Computer, Internet und Smartphone haben unseren Alltag und unser Leben revolutioniert und sich unentbehrlich gemacht. Aber gleichzeitig sind sie auch die Honigfalle der Tyrannei. Die hundertfachen Überwachungsmöglichkeiten aus dem Roman 1984 von George Orwell holen wir uns heute nicht nur selber ins Haus, sondern bezahlen sie auch noch.

Einstweilen ist es wohl am besten, man trocknet den persönlichen Datensee soweit wie möglich aus und verwandelt seine Datenberge in Daten-Müll.

Nur einige, wenige Tipps:

- Schnüfflern und Datensammlern Steine in den Weg legen, wo immer es geht
- wenn es geht und nicht illegal oder rechtswidrig ist, falsche Daten angeben (zum Beispiel Pseudonyme oder falsche Adressen)
- neue Handy-SIM-Karten von anderen Personen anmelden lassen
- Handys und SIM-Karten immer mal wieder mit Freunden tauschen («Tauschkreis»)
- wo es auch immer geht, keine Daten erzeugen und preisgeben
- keine Clouds benutzen
- kurz: mit Daten äusserst geizig umgehen.

Denn merke: Der beste Datenschutz ist immer noch gar keine Daten...

Gerhard Wisnewski

studierte Politikwissenschaften in München. Seit 1986 arbeitet er als hauptberuflicher Journalist, Schriftsteller und Filmautor. Spezialgebiete: Wissenschaft, Technik, Politik und Geschichte. Wisnewski arbeitete für zahlreiche Mainstreammedien wie Bild, Frankfurter Neue Presse, AZ, tz, SZ-Magazin u.v.a.m. Erstes Aufsehen erregte Wisnewski 1992 mit dem Buch Das RAF-Phantom (mit Landgraeber, Sieker). Der darauf beruhende Fernsehfilm erhielt im Jahr 2000 den Grimme-Preis (Regie: Dennis Gansel). Heute gilt Wisnewski als führender Vertreter der Gegenöffentlichkeit und zählt laut «Spiegel» zu den Pionieren «des aktuellen Gegenzeitgeistes».Seit 2008 veröffentlicht er seinen sehr erfolgreichen kritischen Jahresrückblick «verheimlicht – vertuscht – vergessen».

Quellen:

1. chip.de, 22.12.2017
2. Die Welt, online, 10.8.2012
3. Die Welt, online, 19.12.2013
4. Welt/N24, online, 9.6.2017
5. siehe: «How the CIA made Google», medium.com, 22.01.2015
6. Quelle und Übersetzung: netzpolitik.org, 26.8.2014
7. SPD, laut welt.de, 18.11.2010
8. Publicus, Nr. 10/2016
9. netzpolitik.org, 17.10 2014

Internet

Meinungskontrolle durch Google, Facebook, Amazon & Co.

- Internetunternehmen wie Google, Facebook, Twitter, Amazon, Spotify uvm. sind unermüdliche Datenlieferanten, denn jede Nachricht, jeder Klick, jede Suche, jedes Liken etc. ihrer Benutzer wird auf ihren Servern (der «Cloud») gespeichert. Durch die dadurch entstehenden Persönlichkeitsprofile kennen die sozialen Netzwerke und Suchmaschinen die Vorlieben ihrer Nutzer oft besser als deren Umfeld.
- Mit der Weiterentwicklung von Computer- und Internettechnologie wurde eine neue Epoche der Überwachung eingeleitet, denn zum ersten Mal in der Geschichte stimmen die Bürger durch ihre Kaufentscheidung oder Account-Anmeldung der Überwachung zu, sie liefern ihre Daten frei Haus. Der Staat und die Geheimdienste müssen diese Datenflut nur noch abgreifen. So werden wir fast alle zu Komplizen unserer Beobachter.
- Ein historisch neues Mittel der Ausübung von Herrschaft ist auch die Kontrolle des «Rückkanals», also die individuelle Zusammenstellung von Informationen für den Überwachten. Die Internetunternehmen können mittels Personalisierung und Informationskontrolle beeinflussen, was ihre einzelnen Benutzer denken.
- Auch das Denunziantentum, das man heute vor allem mit der DDR und dem Kommunismus verbindet, könnte durch die digitalen Medien wiederbelebt werden: Durch die Ausweitung der bereits bestehenden Online-Bewertungssysteme könnte bald jeder zum potentiellen Richter und Denunzianten seines Nächsten werden. Es droht die totale Sozialkontrolle, wie sie bereits in China durch das staatlich verordnete soziale Bewertungssystem eingeführt wird.

Foto: shutterstock/tanuha2001

Die freiwillige Aufgabe der Freiheit

Die charmanten Tech-Gurus aus Silicon Valley wie Marc Zuckerberg oder Elon Musk sind nicht gerade das, was man sich gemeinhin als «Bösewicht» vorstellt. Sie werden von der breiten Masse nicht als böswillig oder feindselig wahrgenommen. Die Vorstandschefs von Google & Co. sagen sehr freundlich, dass es ihnen um die Verbesserung der Welt gehe. Sie sind smart und elegant. Sie fragen nur nie, ob sie jemand um die Verbesserung der Welt gebeten hat. Heute behauptet der Totalitarismus, die höchste Form der Individualisierung und der Friedfertigkeit darzustellen, die maximale Bequemlichkeit und die grösste Entfernung von Aufwand und Anstrengung. Dieser Totalitarismus kommt daher als Welt, in der für alle gesorgt ist. Die modernen Freiheitsfeinde kommen nicht in Uniformen oder Panzern daher, denn ihr Ziel scheint eine freiwillige Kapitulation der Bürger bzw. ihrer «Kunden» zu sein.

Durch unsere Online-Tätigkeiten fallen riesige Datenmengen an, die sowohl wirtschaftlich wie geheimdienstlich zur Durchleuchtung und Überwachung verwendet werden. Das bedeutet nicht nur, dass der aufwändige Schnüffelapparat der früheren Geheimdienstarbeit ersatzlos gestrichen werden kann, es bedeutet vor allem, dass die Überwachung deswegen lebenspraktisch nicht auffällt, weil sie mit positiv empfundenen Handlungen einhergeht, die der Überwachte selbst initiiert und vollzieht. Weil der Konsument selbst gerne die Angebote nutzt, liefert er auch gern seine Daten. Die dann wiederum zur Verfeinerung seiner Dressur verwendet werden.

Suchmaschinen und Soziale Netzwerke: Unendliche Machtquellen

Wenn 90 Prozent aller Internetnutzer – das sind heute etwa 3,4 Milliarden Menschen – Google benutzen und es mittlerweile 2 Milliarden Facebook-Nutzer gibt, kann man sich in etwa vorstellen, wie gross die Macht dieser Internet-Multis ist: denn jede Nachricht, jede Suche, jeder Klick, jedes Liken, jede Weiterleitung einer Nachricht, jeder Tweet usw. liefert Informationen über alle, die da als unermüdliche Datenlieferanten tätig sind. Hochgeladene Fotos können per Gesichtserkennung zugeordnet, Freundschaftsnetzwerke, Einkaufs- und Mobilitätsgewohnheiten dechiffriert, geheime Vorlieben identifiziert werden.

Natürlich ergibt die Kombination der Überwachungs- und Ausforschungsbedürfnisse von Geheimdiensten mit der uferlosen Datensammelwut von Unternehmen aus kommerziellen Gründen die unheilvollste Allianz, die man sich überhaupt vorstellen kann: Beides zusammen macht die einzelne Bürgerin und den einzelnen Bürger vollkommen wehrlos gegenüber den allfälligen Zugriffsmöglichkeiten auf ihr Inneres von aussen.

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.

Die digitale Dauerbeurteilung

In Ihrem Buch «Die Vernetzung der Welt» kündigen der ehemalige Google-Chef Eric Schmidt und Jared Cohen unverblümt den Beginn einer Gesellschaft an, in der jede unserer Handlungen der Bewertung durch andere ausgesetzt sein wird: «Alle unsere virtuellen Aktivitäten und Beziehungen werden aufgezeichnet, und alles, was wir im Internet abspeichern, wird dauerhaft dort abgelegt. [...] Wir werden für unsere aktuellen und früheren virtuellen Beziehungen zur Rechenschaft gezogen werden. [...] Das Verhalten unserer Bekannten wird positiv oder negativ auf uns zurückwirken. [...] Da Informationen dazu tendieren, ans Licht zu kommen, sollten Sie also nichts abspeichern, das Sie nicht irgendwann in einer Anklageschrift oder auf der Titelseite einer Zeitung lesen wollen, wie es so schön heisst. In Zukunft wird dies nicht nur auf jedes geschriebene und gesprochene Wort zutreffen, sondern auch auf jede Internetseite, die Sie besuchen, auf jeden ‚Freund' in Ihrem Netzwerk, auf jedes ‚Like' und auf alles, was Ihre Freunde tun, sagen und veröffentlichen.» (1) Wenn das exakt von den Leuten verkündet wird, deren Firma die grösste und mächtigste Datenmaschine der Welt ist, klingt das wie eine unverhohlene Drohung, die, übersetzt aus der subjektlosen Technikwunderwelt der Zukunft in die irdische Gegenwart, lautet: «Wir haben Macht über dich, egal wer du bist und wer du zu sein glaubst! Also sieh dich vor!»

Die neue digitale Denunziation

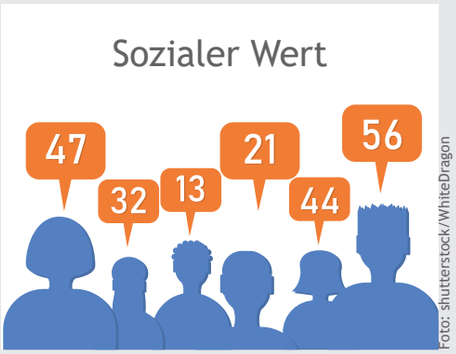


Foto: shutterstock/WhiteDragon

Schmidt und Cohen werden noch deutlicher: «Jede Anwältin, jede Lehrerin und jede Beamtin muss über ihre Vergangenheit Rechenschaft ablegen, wenn sie vorankommen möchte. Was würden Sie davon halten, wenn Ihr Zahnarzt am Wochenende lange Hasstiraden gegen Ausländer ins Internet stellt? Oder wenn der Fussballtrainer Ihres Sohnes nach seinem Studium zehn Jahre lang Touristen durch den Rotlichtbezirk von Bangkok geführt hat? Unser neues Wissen über unsere Kollegen und Führungspositionen wird beispiellose Auswirkungen auf unsere Gesellschaft haben. Die Dokumente aus unserer Vergangenheit werden uns im Alltag und in der Arbeit verfolgen. [...] In demokratischen Ländern wird es im Zeitalter der umfassenden Bürgerbeteiligung schwerer werden, Korruption, Verbrechen und private Skandale zu verbergen.»

Doch sollte der Zahnarzt nicht denken und sagen, was er möchte? Und ich kann entscheiden, ob ich sein Patient sein will oder nicht? Was der Fussballtrainer meines Sohnes nach seinem Studium gemacht hat, geht niemanden etwas an. Und was war an seinem Beispiel überhaupt skandalös? Dass er einen Fuss in einen Rotlichtbezirk gesetzt hat? Und welche Vorstellung soll man sich von «privaten Skandalen» machen? Die Vermutung liegt nahe, und das lassen alle diese Sätze anklingen, dass das Private in der erträumten Zukunft von Schmidt & Cohen selbst der Skandal ist. Niemand soll noch Geheimnisse haben dürfen, niemand eine Vergangenheit oder eine Zukunft, die nicht von den Datendiktatoren kontrolliert ist.

Und folgerichtig kennen sie auch das wichtigste Mittel zur Durchsetzung totalitärer Herrschaft: Jeder wird zum potentiellen Richter und Denunzianten seines Nächsten: «In einer Demokratie, in der freie Meinungsäusserung und Bürgerbeteiligung zu Veröffentlichungen ermuntern, werden Bürger zunehmend zu Richtern ihrer Mitbürger. Je mehr Daten über jeden Menschen verfügbar sind, umso stärker wird dieser Trend», so Schmidt und Cohen.

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.
1. Eric Schmidt, Jared Cohen: Die Vernetzung der Welt. Ein Blick in unsere Zukunft. Reinbek bei Hamburg 2013, S.28

Vom neuen Bewertungskult zum sozialen Kreditsystem?

In der Sendung «Von Daten verraten» des SRF vom 30. August 2017 wurde ein Blick auf die Kehrseite der digitalen Welt und den Preis an Privatsphäre, den wir dafür bezahlen, geworfen. «Nicht Kleider, sondern Klicks machen Leute», so sei das heute.

Das SRF fragt sich, wie die Digitalisierung das gesellschaftliche Miteinander, den Menschen als soziales Wesen, beeinflusst. Um der Antwort auf die Spur zu kommen, liess es den Berliner Soziologen Steffen Mau zu Wort kommen: «Es gibt Schätzungen, die sagen, dass wir ungefähr 4.800 Mal am Tag sozusagen über Kommunikation mit dem Internet oder mobilen Geräten, Daten abgeben, und das betrifft letzten Endes alle Lebensbereiche.»

Weiter erklärt Mau, wie solche Daten weltweit systematisch gesammelt und ausgewertet werden: «Es gibt zum Beispiel eine grosse amerikanische Firma, Acxiom heisst die, die hat ein eigenes Datensystem, die treten als (sogenannte) Datenbroker auf, die haben zum Beispiel über viele hundert Millionen Menschen weltweit, auch in Europa, Daten gesammelt.»

Foto: SRF

Das SRF ergänzt, wie diese Datenbroker – auch Informationsvermittler genannt – aus der Fülle der Datenströme herausfiltern, welche Informationen zu welchem Menschen gehören. Daraus werde dann Punkt um Punkt ein Persönlichkeitsprofil errechnet, sozusagen ein digitaler Zwilling. Das Sozialwesen Mensch werde permanent vermessen und entsprechend bewertet. Besonders tückisch sei es, wenn sogenannte Emojis z.B. in Facebookprofilen genutzt werden. Bei Facebook habe ein internes Papier den Weg an die Öffentlichkeit gefunden, in dem die Firma darüber nachgedacht habe, dass Jugendliche, die häufig «traurig» sind, als Zielgruppe an Werbekunden der Pharmaindustrie weiterverkauft werden könnten. Auch an diese Tatsache, dass Daten zu Werbezwecken weitervermittelt werden, dürften sich wohl die meisten Menschen gewöhnt haben.

Foto: SRF

Der Soziologe Steffen Mau sieht im Wettbewerb zwischen guten und schlechten Daten einen gefährlichen Türöffner für ein totalitäres, staatlich verordnetes soziales Bewertungssystem.

Die Gefahr der sozialen Vergleiche

Nun wird es aber interessant: Soziologe Mau sieht darüber hinaus Gefahren mit weit grösserer Tragweite: «Wenn Sie Daten haben, dann werden diese Daten genutzt, um soziale Vergleiche anzustellen, Vergleiche zwischen Individuen und zwischen Universitäten, zwischen Krankenhäusern, wie auch immer. Also Daten führen zu einer Universalisierung von Vergleich und zugleich zu einer Verbreitung von Wettbewerb. […] Die führen eben dazu, dass es eine neue Form von Statusordnung gibt, wo diejenigen, die gute Daten haben und mit guten Zahlen glänzen, eben oben stehen, und diejenigen, die schlechte Werte haben oder schlechte Daten, weit unten stehen.»

Dieser neue Bewertungskult könne z.B. genutzt werden, wenn Unternehmen Personen einstellen oder Wohnungsinteressenten an Vermieter vermittelt werden, d.h. eine Selektion von Personen in «gute» und «schlechte», oder in solche, die den jeweiligen Ansprüchen gerecht werden oder eben auch nicht, stattfindet.

Das soziale Kreditsystem

Denn, wie das SRF folgert, besonders bedenklich sei die Entwicklung in China. Das staatlich verordnete soziale Bewertungssystem erfasse alle Online-Aktivitäten vom Chat bis zum Shopping, aber auch Finanz- und Strafregisterdaten. Pluspunkte gebe es für regierungstreues Verhalten und gute Zahlungsmoral. Abzug gebe es für oppositionelle Äusserungen oder für einen verschwenderischen Lebensstil. Freunde mit schlechten Zahlen drücken ebenfalls auf den eigenen Wert. Bürger mit niedrigen Werten gelten dann als unverantwortlich und demzufolge als nicht würdig, Kredite, Hotelzimmer oder Reisegenehmigungen zu erhalten. Es drohe die totale Sozialkontrolle, so die Kulturplatz-Sendung des SRF.

Foto: SRF

Läuft es darauf hinaus, dass Menschen mithilfe digitaler Daten ausgegrenzt werden sollen? Ist diese totale Sozialkontrolle bis hin zur Ausgrenzung wirklich nur in China relevant, wie die Sendung des SRF unterschwellig vermittelt? Das SRF wird sich dessen sicher bewusst sein, dass es gerade in unseren Breitengraden tendenziell dahin läuft, dass Menschen, die sich nicht system- oder regierungskonform verhalten, benachteiligt und ausgegrenzt werden. Ist es nicht so, dass diese Entwicklung der Benachteiligung und Ausgrenzung «politisch unkorrekter» Personen besonders auch in vorgeblich demokratischen westlichen Ländern schon längst gängige Praxis ist?

Nicht-systemkonforme Menschen können mithilfe digitaler Daten besser geortet, bestraft, benachteiligt oder ausgegrenzt werden – seien es Medien- oder Systemkritiker, Gegner der Frühsexualisierung oder Abtreibungsgegner, Verweigerer von gentechnisch veränderten Lebensmitteln, Impfungen oder eines RFID-Chips unter der Haut; Kriegsgegner usw.

Quelle: kla.tv, Warum die Gefahr der Digitalisierung kalt lässt, 06.10.2017

Foto: Matt Shirk (https://commons.wikimedia.org/wiki/File:Online_Privacy_and_the_Founding_Fathers.jpg) https://creativecommons.org/licenses/by-sa/4.0/deed.en

Keine Freiheit ohne Privatsphäre

Der Bürger wird substantiell entmachtet, wenn die Privatheit durch Dauerüberwachung und ein allumfassendes Bewertungssystem abgeschafft wird: Freiheit setzt nämlich schlicht und einfach voraus, dass es Bürgerinnen und Bürger gibt, die für ihre Angelegenheiten und das Gemeinwesen eintreten und es gestalten. Das können sie aber nur dann, wenn es eine Trennung von öffentlich und privat gibt: Ich kann nur dann Bündnisse schliessen, Strategien entwickeln, Argumente verfertigen, wenn es einen privaten Raum gibt, in den niemand Einblick hat. Dasselbe gilt für meine Person.

Ich bin nur dann autonom, wenn ich Dinge tun oder lassen kann, ohne irgend jemand anderem darüber Rechenschaft abzulegen. Alle Verfassungsväter der amerikanischen Verfassung waren sich der Notwendigkeit des absoluten Schutzes von Privatheit bewusst, deshalb stehen Grundrechte wie die Unverletzlichkeit der Wohnung, das Briefgeheimnis usw. in jeder modernen Verfassung.

Und genau deshalb waren sich alle totalitären Denker und Herrscher und Diktatoren darüber klar, dass Privatheit das zentrale Hindernis für die Durchsetzung totaler Herrschaft ist. Solange Menschen etwas für sich haben, in das niemand anderer, schon gar nicht der Staat, eindringen kann, sind sie nicht vollständig beherrschbar. Deshalb ist in allen Diktaturen «das Selbst das erste besetzte Gebiet.»

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.

Die Kontrolle des Rückkanals

Jaron Lanier, einer der klügsten Vertreter der Internetszene, spricht von Nutzern, die «dressiert werden, sich den Regeln von Facebook und anderen Netzwerken zu unterwerfen, so dass sie in ständiger Furcht leben, die empfundenen Vorzüge des Netzes zu verlieren, wenn sie sich nicht konform verhalten. [...] Facebook ist kein Medienhaus, Facebook ist ein Konzern der Verhaltenskontrolle. [...] Das Entscheidende ist, den Rückkanal für Informationen zu erobern, ihn feinfühlig zu manipulieren und darüber Verhalten zu beeinflussen.»

Das ist ein historisch neues Mittel der Ausübung von Herrschaft. Denn einen «Rückkanal» gab es in Diktaturen, wie wir sie kannten, nicht. Herrschaft bedurfte zwar der Zerstörung von Privatheit durch Überwachung, Denunziation und Spitzelwesen, auch der Androhung und Anwendung von Gewalt, aber im Unterschied zu heute konnte diese Herrschaft nicht mittels Personalisierung und Informationskontrolle bestimmen, was die Beherrschten selbst zu sein glaubten und sein wollten. Die Beherrschung des Rückkanals ist eine entscheidende machttechnologische Innovation.

> Die glücklichen Sklaven sind die erbittertsten Feinde der Freiheit.»
>
> *Marie Ebner von Eschenbach, österreichische Schriftstellerin*

Foto: shutterstock/Pressmaster

Personalisierung: Überwachung und Dressur in einem

Der Musikstreamingdienst Spotify, der 75 Millionen Nutzer hat, erfasst, wie seinen Geschäftsbedingungen zu entnehmen ist, «Informationen, die Sie auf Ihrem Mobilgerät gespeichert haben. Dazu gehören Kontakte, Fotos und Mediadaten.» Wozu erfasst Spotify das alles, wenn man doch nur das neueste Stück des Lieblingskünstlers hören möchte? Wenn man sich früher eine Schallplatte gekauft hat, wollte die Deutsche Grammophon doch auch nicht wissen, was man so machte, wenn man gerade nicht Musik hörte. Die Antwort: «Ziel ist es, den Kunden in möglichst vielen Alltagssituationen die jeweils passenden Musikvorschläge zu unterbreiten. So bietet der Musikdienst an, beim Joggen den Rhythmus der Musik an das Lauftempo anzupassen. Dafür braucht er Daten darüber, wie sich der Nutzer bewegt.» Na klar. Man stelle sich bloss vor, der Jogger würde seine Musik selbst aussuchen, und dann passt sie gar nicht.

Das nennt man Personalisierung. Eli Pariser hat dazu das Wesentliche in seinem Buch «Filter Bubble» geschrieben, in dem er nachzeichnet, wie Facebook, Google und viele andere die umfassende Datensammlung über Sie wiederum in massgeschneiderte Informationsangebote für Sie übersetzen. Das Prinzip ist einfach und von Amazon bekannt: Jede Informationssuche und jeder Kaufakt ist zugleich eine kommerziell höchst interessante Information, die sofort für eine Empfehlung verwendet werden kann. Daher werden Sie regelmässig von Amazon mit Informationen zu Büchern versorgt, die entweder andere Kunden auch angesehen oder gekauft haben oder von denen Amazons Algorithmus berechnet hat, dass sie Sie interessieren müssten. Es kann auch sein, dass jemand dafür bezahlt hat, ein Werk in Ihrer Vorliebensliste zu platzieren, das liegt in der Natur der Sache.

Das zugrundeliegende Prinzip, aus protokollierten Verhaltensmustern Prognosen für künftiges Kauf- oder Buchungsverhalten abzuleiten, gilt seither überall im Netz – egal ob Ihnen ungefragt Hotels, Reisen, Möbel, Mixgeräte, Ärzte, Medikamente, Partnerinnen oder Partner empfohlen werden. Immer orientiert sich das Angebot an einer Information, die der Anbieter über Sie hat. Das kann auch sehr direkt gehen. Die niederländische Fluggesellschaft KLM hat 2010 unter grossem Beifall ihren Gästen kleine Geschenke überreicht: «Eine Pulsmessungsuhr für die Frau, die Berge besteigen, einen New-York-Führer für jemanden, der New York erkunden wollte. Personalisierte Geschenke, ermöglicht durch die Kombination von Twitter und Facebook, wo KLM erfuhr, wer demnächst mit welchem Reisegrund und mit welchen persönlichen Interessen in ihren Flugzeugen sitzt. Eine Kampagne von grossem Erfolg, die KLM das Attribut der Coolness und der Medienkompetenz einbrachte.»[1]

Die Frankfurter Allgemeine Zeitung berichtete am 04. August 2015 von einer Studie des französischen Sicherheitsunternehmens Eurecom, das testweise 2000 Gratisapps aus 25 verschiedenen Kategorien im Google Play Store geladen und dann den Netzwerkverkehr der Apps analysiert hatte. Das Ergebnis: Die Programme steuerten «heimlich insgesamt 250 000 verschiedene Webadressen an und gaben Daten weiter. Der Spitzenreiter ist Music Volume EQ, eine Equalizer-App zur akustischen Klangeinstellung, die sich im Hintergrund mit 2000 Servern verbindet.» Die Fachzeitschrift «c't» hat dem-

selben Artikel zufolge die Programme der 50 beliebtesten Gratis-Apps in Deutschland analysiert und festgestellt, dass lediglich zwei davon keine Informationen an Werbenetzwerke sendeten. (2)

In der Tat: Wenn man sich anschaut, was alles als Information gegen Sie zu Entmündigungszwecken verwendet werden kann, wird man blass. Sie verfügen beim Lesen von E-Books über Funktionen wie das Markieren von Textstellen, das Hinterlassen von Anmerkungen, das Kniffen von Eselsohren. Wenn Sie sie benutzen, füttern Sie die Datenabsaugmechaniken mit noch genaueren Details zu ihren Lesepräferenzen, ebenso wie Ihre Auswahl von Filmen bei Netflix nicht nur wichtige Informationen für deren massgeschneidertes Angebot für Sie liefert, sondern für die Erfolgswahrscheinlichkeit künftiger Filmproduktionen überhaupt.

Wahlbeeinflussung durch Internetmedien

Auch politisch betrachtet tut sich mit der Personalisierungstechnologie ein ganz neues Universum manipulativer Möglichkeiten auf. Einfach gesagt: Wenn ich die politischen Präferenzen von Bürgerinnen und Bürgern personalisiert kenne, ergeben sich ganz neue Möglichkeiten des Einmassierens von Botschaften in die Hirne: Für Nichtwähler nehme ich tunlichst eine andere Strategie der Ansprache als für Anhänger einer bestimmten Partei, für Abtrünnige und Wechselwähler wiederum eine andere. Das Wahlkampfteam von Barack Obama war bekanntlich das erste, das die Internetmedien systematisch für die Wähleransprache und –gewinnung eingesetzt hat, mit grossem Erfolg.

Damals wusste man aber noch wesentlich weniger über die individuellen Wählerinnen und Wähler als heute. Wenn sich, wie heute, jeder dritte Amerikaner über Facebook informiert, dann können unglaubliche effektive Strategien nicht in der Wahlbeteiligung, sondern auch der Entscheidung für oder gegen einen Kandidaten entwickelt werden. «Die Verhaltensforscher Robert Epstein und Ronald E. Robertson vom American Institute for Behavorial Research and Technology konfrontierten Probanden mit vorab verzerrten Suchmaschinenergebnissen über die australischen Parlamentswahlen. Diese wurden als Objekt gewählt, weil die Forscher annehmen konnten, dass die Versuchsteilnehmer

Foto: shutterstock/Cienpies Design

das politische System Australiens kaum kannten und ein relativ unvoreingenommenes Bild der Kandidaten hatten. Epstein und Robertson wollten herausfinden, ob die Information einen Einfluss auf die Präferenzbildung ausübt. Der ersten Gruppe wurden Suchergebnisse angezeigt, die die damalige Amtsinhaberin Julia Gillard favorisierten; der zweiten wohlwollende Ergebnisse über den Herausforderer Tony Abott, der Kontrollgruppe neutrale Inhalte. Ergebnis: Diejenigen, die parteipolitisch gefärbte Inhalte sahen, hatten später eine deutlich positivere Einstellung gegenüber dem Kandidaten als die neutrale Gruppe. Auch die Wahlpräferenz änderte sich zugunsten der Kandidaten. Das zeigt: Suchmaschineneinträge können Wählerpräferenzen steuern.» (3)

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.
1. Roberto Simanowski, Data Love, 2014
2. FAZ, 04.08.2015, S.14.
3. FAZ, 06.08.2015, S.13

Bestseller-Autor Harald Welzer legt mit «Die smarte Diktatur. Der Angriff auf unsere Freiheit» eine neue und frische Analyse der grossen gesellschaftlichen Zusammenhänge in Deutschland vor, eine umfassende Diagnose der Gegenwart für alle politisch Interessierten. Nach seinem Bestseller «Selbst denken» analysiert Harald Welzer, wie die scheinbar unverbundenen Themen von Big data über Digitalisierung, Personalisierung, Internet der Dinge, Drohnen bis Klimawandel zusammenhängen.

Facebook kennt Nutzer besser als eigene Familie

Like

Psychometrie ist der wissenschaftliche Versuch, die Persönlichkeit eines Menschen zu vermessen. In der Psychologie nutzte man dafür Fragebogen-Methoden, mit der sich Charakterzüge messen lassen, z.B. welche Bedürfnisse und Ängste der jeweilige Mensch hat, aber auch wie er sich höchstwahrscheinlich verhalten wird. Ein Problem dabei war, Menschen zur Preisgabe ihrer persönlichen Ansichten zu bewegen, doch das änderte sich mit dem Aufkommen des Internets, wo zahlreiche Nutzer freiwillig und unbedacht ihre persönlichsten Daten veröffentlichen. Der Psychometrie-Spezialist Michal Kosinski entwickelte ein Verfahren, mit dem er erfragte Werte von Test-Personen mit allen über sie verfügbaren Onlinedaten abgleicht. Er bewies, dass man alleine aus durchschnittlich 68 Facebook-Likes eines Nutzers mit bis zu 95-prozentiger Sicherheit seine Hautfarbe, Intelligenz, Religionszugehörigkeit, sexuelle Neigung sowie seinen Alkohol-, Zigaretten- und Drogenkonsum berechnen kann. 150 Likes geben laut der Studie mehr preis, als die eigene Familie weiss. Da die Persönlichkeitsprofile vieler Menschen durch Facebook & Co. derart leicht ermittelt werden können, hat nicht nur die Werbeindustrie bei der Manipulation ihrer Zielgruppe ein leichtes Spiel, sondern die Steuerung und Beeinflussung der Menschen wird allgemein immer leichter. Willkür und Missbrauch stehen Tür und Tor offen!

Quelle: Stimme Und Gegenstimme 36/17
tagesanzeiger.ch, Diese Firma weiss, was Sie denken

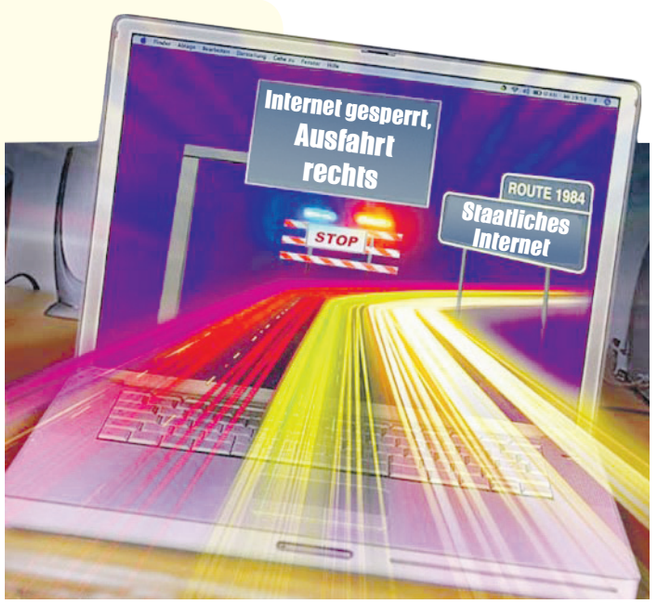
WhatsApp

Facebooks Veruntreuung persönlicher Daten

2014 kaufte der Gründer von Facebook, Mark Zuckerberg, den Kurznachrichtendienst WhatsApp für 19 Mrd. Euro auf, um seinen Facebook-Nutzern einen beinahe kostenlosen Nachrichtenaustausch zu ermöglichen. Im Januar 2017 wird dieser Dienst bereits von 1,2 Mrd. Menschen weltweit genutzt. Mit Facebook in Kooperation mit WhatsApp schuf Zuckerberg einen medialen Riesen, doch mit Schattenseiten. Über alles, was auf Facebook eingestellt wird, hat die Firma das Copyright. Zudem räumt der Nutzer von WhatsApp ein, dass Telefonnummern von Kontaktdaten, die im Adressbuch des Nutzers gespeichert sind, an Facebook weitergegeben und genutzt werden dürfen. «Wir verfolgen einige deiner Handlungen auf Facebook», gibt Zuckerberg verharmlosend zu. Die erfassten Daten würden u.a. zur besseren Personalisierung von Werbung genutzt. Diese Ausbeute der persönlichen Daten bringt Facebook-Gründer Zuckerberg aber einen gigantischen Zufluss an Profit ein. Aber auch Anfragen von Regierungsstellen über Nutzer bleiben von Facebook nicht unbeantwortet. Eine fast unüberschaubare Möglichkeit an Überwachung wird zu Lasten der arglosen Nutzer ausgeschöpft. Wurde Facebook auf dieses Ziel hin vielleicht sogar gegründet?

Quellen: Stimme und Gegenstimme 31/17
Zeitenschrift.com, Facebook is watching you

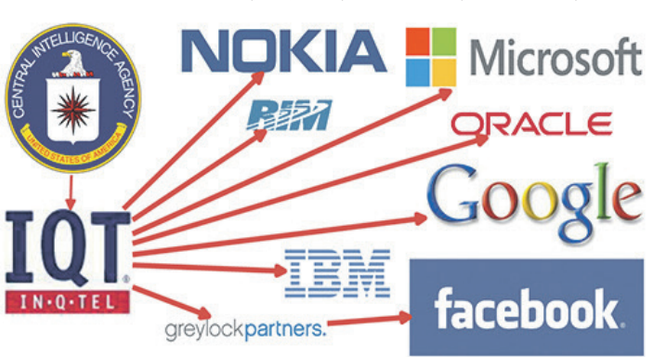
Trojanische Pferde des Staates?



Wie auch Tesla (siehe S. 39), gehören die Internet-Riesen zu den strategischen Neugründungen des US-Imperiums, die zu wichtig sind, um sie dem Zufall oder dem freien Markt zu überlassen: Microsoft, Apple, Facebook, Wikipedia, YouTube, Amazon und andere mehr. Sie alle dienen dem einen Ziel, nämlich Know-how und Technologien zu monopolisieren, den Wettbewerb plattzumachen und anschliessend ganze Märkte und letztlich die Welt zu beherrschen. Man stelle sich nur einmal vor, in Zukunft nur noch bei Amazon einkaufen zu können. Was wird uns dann wohl blühen? Aber genau darauf arbeitet dieses Unternehmen hin. Und auch Amazon wird schliesslich massiv staatlich subventioniert, und zwar durch grosszügig geduldete Steuerflucht. Oder sollte man sagen: durch staatlichen Steuerverzicht? Nur so kann es sein explosionsartiges Wachstum finanzieren.

Wagniskapital von der CIA

Denn all diese Mega-Konzerne gehören zur globalen Staatsräson und zur globalen strategischen Planung, wonach es nur noch allmächtige Monopole geben soll. Alles und jedes ist dann unter Kontrolle. Aber nicht doch: Das sind doch alles Verschwörungstheorien! Dieses Bild ändert sich schnell bei genauerem Blick auf eine CIA-Firma, von der Sie bestimmt noch nie etwas gehört haben, nämlich von In-Q-Tel. Denn ob Sie es glauben oder nicht: Die CIA vergibt systematisch Wagniskapital und investiert in futuristische Firmen in den Bereichen Software, Biotech, Elektronik, Hardware, Sensoren und anderen mehr. Mit anderen Worten fördert In-Q-Tel sogenannte «James-Bond-Technologien», woher auch der Firmenname rührt – nämlich von dem legendären Bond-Ingenieur «Q».



Laut Washington Post «hat praktisch jeder US-Unternehmer, -Erfinder oder -Wissenschaftler, der sich mit der Analyse von Daten beschäftigt, schon einmal einen Anruf von In-Q-Tel bekommen oder wurde von seinem Mitarbeiterstab gegoogelt» (15.08.2005). Und wenn In-Q-Tel nicht anruft, fragen viele High-Tech-Erfinder in den USA von sich aus bei dem CIA-Unternehmen nach, ob dort nicht Interesse an ihrer Erfindung und einem Investment bestünde. Den Business-Plan kann man angeblich ganz einfach auf der In-Q-Tel-Website hochladen. Logischerweise können die Technologien anschliessend auch von der CIA genutzt werden: Schon im Jahr 2005 hatte In-Q-Tel laut Washington Post «in mehr als 75 Unternehmen investiert und der CIA mehr als 100 Technologien eingebracht, von denen die meisten sonst nicht einmal von der Behörde in Erwägung gezogen worden wären.»

Mit anderen Worten: Die CIA mausert sich klammheimlich zu einer Holding für lauter kleine und grössere Unternehmen, die einem James Bond und einem Mister «Q» zur Ehre gereicht hätten. Dazu sollen beispielsweise auch Google und Facebook gehören – zwei Konzerne, die praktisch alles über uns wissen, insbesondere über diejenigen, die dort ihr Privatleben eintippen: «Wie die CIA Google machte» lautete

beispielsweise eine Überschrift auf der Nachrichten-Website medium.com. Dort wurde eine gewisse Dr. Bhavani Thuraisingham zitiert, die in den 90er-Jahren des zurückliegenden Jahrhunderts ein gewaltiges Datenprojekt für die CIA, NSA und das zentrale Direktorium der Geheimdienste geleitet haben soll. Dabei habe man über den Computerwissenschaftler Jeffrey Ullman «einige vielversprechende Studenten» unterstützt: «Einer von ihnen war Sergey Brin, der Gründer von Google». (1)

Keine NSA ohne Google

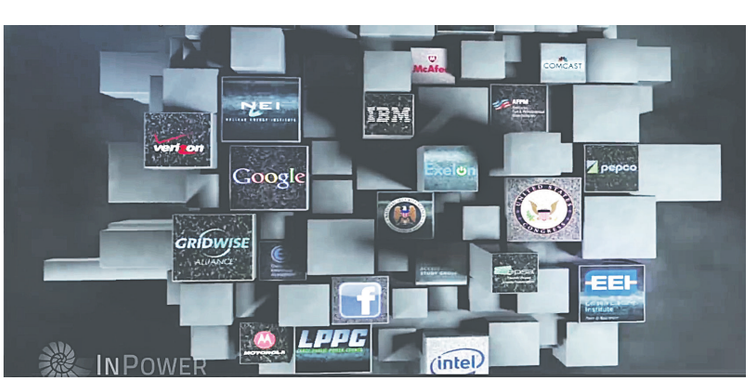
Dass die NSA invasiv Daten dieser Unternehmen abschöpft, ist mittlerweile kein Geheimnis mehr. So gestand ein Mitarbeiter ein: «98 Prozent der PRISM-Ergebnisse beruhen auf Yahoo, Google und Microsoft, wir müssen sicherstellen, dass wir diesen Quellen keinen Schaden zufügen.»

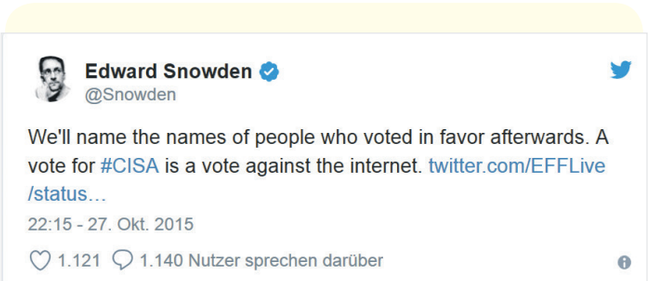
Der hegemoniale Zugriff der NSA auf alles, was sich im Bereich elektronischer Kommunikation abspielt, geht historisch darauf zurück, dass der Ursprung des Internets in den USA liegt und der grösste Netzwerkhersteller Cisco und der grösste Cloud-Anbieter Amazon dort ihre Sitze haben. «Google, Amazon, Ebay, Skype, Apple, Microsoft, Facebook & Co. sind Firmen, die Standards setzen und den Markt beherrschen. Die digitale Dominanz amerikanischer Dienste und Konzerne ist erdrückend. Im Netz sind die USA immer noch eine unangefochtene Supermacht.» (2)

Das hat es historisch noch nicht gegeben: Denn zu früheren Zeiten waren Geheimdienste und Geheimpolizeien noch darauf angewiesen, die Daten, die sie zur Ausforschung der Bürgerinnen und Bürger benötigten, selbst über Einbrüche, Lauschangriffe, Anheuern von Spitzeln, Belohnung von Denunzianten, verdeckte Ermittler usw. zu erheben. Heute liefern sie den Diensten alles frei Haus. Organisationen wie die NSA, der BND und alle anderen müssen diese Datenflut nur noch in ihre Kanalisationssysteme leiten. Das macht alle zu Komplizen ihrer eigenen Überwachung.

CISA-Gesetz: Weitergabe von Nutzer-Informationen an Geheimdienste legal

Der US-Senat hat im Oktober 2015 den umstrittenen Cybersecurity Information Sharing Act (CISA) mit 74 zu 21 Stimmen verabschiedet. Er soll zur Verhinderung von «Cyberangriffen» auf die amerikanische Wirtschaft den Datenaustausch zwischen Unternehmen und





Whistleblower Edward Snowden bezeichnete das CISA-Gesetz auf Twitter als das «Ende des Internets».

Behörden ermöglichen. Bürgerrechtsgruppen und IT-Firmen bemängeln, dass persönliche Daten unkontrolliert an Regierungsbehörden weitergeleitet werden, und sehen das Gesetz als eine weitere Überwachungsmassnahme.

Mit CISA erhalten Unternehmen rechtliche Immunität für die Datenweiterleitung. Verschiedene Regierungsbehörden, u. a. das Heimatschutz-, das Verteidigungs- und das Justizministerium bekommen die Informationen, darunter sensible Daten von Nutzern, automatisch übermittelt. Diese können sie ebenfalls mit anderen Ermittlungsbehörden und Geheimdiensten teilen, welche die Daten auch für andere Zwecke nutzen dürfen. (3)

Politisch korrekte Zensur im Sinne der Mächtigen

Zwar arbeiten Regierungen aller Welt mit Hochdruck daran, die Meinungsfreiheit im Internet durch Zensurgesetze einzuschränken, doch massive Manipulations- und Zensurskandale der Vergangenheit legen den Verdacht nahe, dass Google, Facebook & Co. schon längst als vorgeschobene Propaganda-Werkzeuge der Regierungen agieren.

Nur eines von Dutzenden Beispielen: In einer verdeckten Video-Untersuchung des Investigativ-Portals «Project Veritas» stehen aktuelle und ehemalige Twitter-Mitarbeiter vor der Kamera und erklären Schritte, die der Social-Media-Riese unternimmt, um politisch unerwünschte Inhalte zu zensieren. Am 3. Januar 2018 erklärte ein ehemaliger Twitter-Software-Entwickler [...], dass Twitter eine Strategie, die als «shadow banning» (heimliches Sperren) bezeichnet werden kann, anwendet.

Der Gesperrte soll nicht wissen, dass er gesperrt wurde. Er soll weiterhin Beiträge schreiben, die keiner sieht. Der Gesperrte denkt dann, niemand würde sich mit seinen Kommentaren beschäftigen, während sie in Wirklichkeit niemand sehen kann.

Seite 17

Ein ehemaliger Twitter-Ingenieur bestätigte am 1. Dezember 2017, dass bereits Werkzeuge angewendet werden, um Pro-Trump- oder konservative Inhalte auf der Plattform zu zensieren. Auf die Frage nach dem Prozess der Sperrung wurde von einem Twitter-Inhaltsüberwacher erklärt: «Bei solchen Dingen war es mehr unser Ermessen und unser Standpunkt, wie man eine bestimmte Angelegenheit gesehen hat. [...] Wenn es ein Pro-Trump-Kommentar war und ich bin Anti-Trump [...] dann habe ich den gesamten Account gesperrt [...] es liegt in meinem Ermessen.»

Ein Mitarbeiter erklärte, dass es sich bei diesem Auswahlverfahren nicht exakt um eine Twitter-Politik handelte, sondern um ungeschriebene Regeln von oben: «Viele ungeschriebene Regeln, und da wir in San Francisco sind, in Kalifornien, sind wir sehr liberal, ein sehr demokratischer Staat. [...] Ich meine, als Firma kannst du es nicht wirklich zugeben, weil es dich schlecht aussehen lassen würde, aber hinter verschlossenen Türen gibt es viele Regeln...Es gab, würde ich sagen...Twitter war wahrscheinlich ungefähr 90% Anti-Trump, vielleicht zu 99% Anti-Trump.»

Quellen: Gerhard Wisnewski; Verheimlicht, Vertuscht, Vergessen 2018, Kopp Verlag, Rottenburg.
Bürger für Bürger, Ausgabe 49, März 2018
1. «How the CIA made Google», medium.com, 22.01.2015
2. Marcel Rosenbach, Holger Stark: Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung, München 2015, S.117
3. netzpolitik.org, CISA: Ein als «Cybersecurity» getarntes Überwachungsgesetz, 28.10.2015

Rund-um-die-Uhr-Belauschung durch «Smart Speaker»

Sie beantworten Fragen nach dem Wetter, erzählen Witze, lesen Kalendereinträge vor oder stellen einen Timer; beantworten Wissensfragen wie, wann wer gestorben ist, nennen den Aktienkurs eines Unternehmens oder verbinden sich mit einem Wikipedia-Artikel. Oder sie greifen über einen Musikservice wie Spotify, Amazon Music oder Google Play auf Millionen von Songs zu, spielen sie ab, sobald man Titel oder Interpret nennt: Die neuen «Smart Speaker», mit dem Internet verbundene Lautsprecher, die durch Spracherkennung das Leben ihrer Besitzer erleichtern sollen.

Amazons «Echo» kann sich auch über Bluetooth mit dem Smartphone verbinden und dort Musik abspielen; eine Funktion, die künftig auch bei «Google Home» verfügbar sein soll. Die Google-Variante in Lautsprecherform kann auch auf Chromecast-Adapter zugreifen, beispielsweise an Lautsprechern und TV-Geräten, und diese dann zum Beispiel mit Youtube und Netflix verbinden.

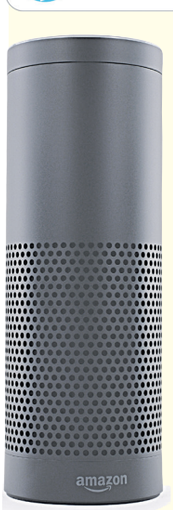


Foto: Frmorrison at English Wikipedia

Der «Amazon Echo»-Lautsprecher, greift auf den intelligenten digitalen Assistenten «Amazon Alexa» zu.

USA schon weit voraus

Da sowohl Amazon als auch Google ihre Assistenten für fremde Entwickler öffnen, die dafür Anwendungen programmieren, gibt es für Amazon bereits 1.600 unterschiedliche Fähigkeiten in Deutschland und etwa zehnmal so viele in den USA. Google Home stehe hier erst am Anfang, so die «Welt».

«Amazon Echo»-Nutzer können in den USA bereits mit anderen «Echo»-Nutzern über die Geräte Gespräche führen, «Google Home» greift sogar auf andere Telefone zu. Derzeit habe Amazon hier klar die Nase vorn. Doch Google verfüge über deutlich mehr Nutzerdaten, die in individuelle Dienste umgesetzt werden können, so das Blatt weiter.

Big Brother - die andere Seite

Am Beispiel Amazon Echo/Alexa wird jedoch deutlich, wie gefährlich das neue Wunder sein kann, denn alle «Sprachbefehle und Sprachbotschaften werden dauerhaft in der Amazon-Cloud (d.h. Server von Amazon) gespeichert, um die Spracherkennung zu verbessern», heisst es auf Wikipedia.

US-Journalisten hätten beim FBI angefragt, ob «Amazon Echo» zum Abhören benutzt werden könne. Dies wurde weder bestätigt noch dementiert. Im Dezember 2016 hätten Behörden jedoch bereits erstmals offiziell auf Cloud-gespeicherte Audio-Daten zugegriffen, um Hinweise in einem Mordfall zu erhalten, berichtete die CBS-Tochter «CNET».

Andrea Vosshoff, Bundesbeauftragte für den Datenschutz, gab laut «Wirtschafts-Woche» zu bedenken: «Ich sehe intelligente Sprachassistenten, die mit einem Mikrofon permanent ihre Umgebung belauschen, erst mal kritisch. [...] Ich rate allerdings, eine solche Entscheidung gut zu überdenken [...] und den Komfortgewinn durch die Nutzung des Sprachassistenten gegen eine – jedenfalls theoretische – Rund-um-die-Uhr-Überwachung der Privatsphäre abzuwägen.»

Der kleine Lautsprecher «Google Home» in Grösse einer Kaffeetasse wird per Smartphone-App eingerichtet und über Wlan mit dem Internet verbunden. Er reagiert auf Zuruf und greift dabei auf den digitalen «Google Assistant» zu.

Foto: NDB Photos (https://commons.wikimedia.org/wiki/File:-Google_Home_sitting_on_table.jpg) https://creativecommons.org/licenses/by-sa/2.0/deed.en

Foto: Rick4512 (https://commons.wikimedia.org/wiki/File:An_Apple_HomePod_speaker_.png) https://creativecommons.org/licenses/by-sa/4.0/deed.en

Der Homepod von Apple greift auf den digitalen Assistenten Siri zu.

Da die Smart Speaker durch ein Sprachsignal wie z.B. «Hey Alexa» oder «Hey Google» aktiviert werden können, muss das Mikrofon die ganze Zeit eingeschaltet bleiben. Ein jederzeit eingeschaltetes Mikrofon ist bedenklich, da es bedeutet, dass das Gerät Sie und andere Personen in der Nähe potenziell abhören kann.

Quelle: epochtimes.de, Gefangen im digitalen Netz: «Google Home» jagt Amazons «Alexa» – Als Menschen ihre Freiheit gegen Bequemlichkeit tauschten, 20.07.2017

Die Mikrofone der smarten Lautsprecher lauschen allzeit bereit auf das Aktivierungswort und vielleicht auf noch mehr, wie es hier (noch?) überspitzt dargestellt wird.

Fotos: ARD

Googles Eric Schmidt: Chip im Gehirn, wenn die Technologie besser wird?

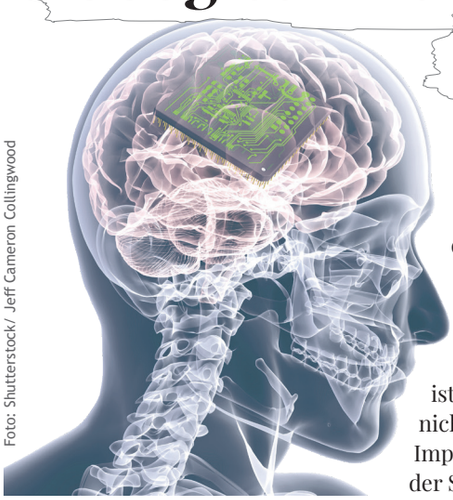


Foto: Shutterstock/ Jeff Cameron Collingwood

In einem Gespräch mit einem Reporter liess Eric Schmidt kurz aufblitzen, welches ethische Verständnis in den höheren Etagen der Tech-Konzerne vorherrschend zu sein scheint:

Eric Schmidt: «Da ist etwas, das wir die ‚Schmerzgrenze' nennen. Und die Google Richtlinie bezüglich vieler dieser Themen ist, bis zur Schmerzgrenze zu gehen, aber nicht darüber hinaus. Ich würde sagen, dass das Implantieren von Geräten im Gehirn jenseits der Schmerzgrenze liegt.»

Reporter: «Besonders in meinem.»

Eric Schmidt: «Ja, zumindest im Moment... bis die Technologie besser wird.»

Schmidt sagt, dass Googles Schmerzgrenze nur durch den heutigen Stand der Technologie definiert wird? Was hat denn ein höherer Stand der Technologie mit Moral oder Ethik zu tun? Das ist ein deutlicher Hinweis darauf, dass Pietät und moralische Grenzen für die Oberschicht des Silicon Valley kaum eine Rolle spielen. Wollen wir diesen Leuten wirklich all unsere Daten anvertrauen?

RFID

RFID-Technologie:

RFID-Funketiketten/RFID-Chips sind Datenträger, die zur Identifikation dienen, ähnlich dem altbekannten Barcode. Der Vorteil der RFID-Chips im Vergleich zum Barcode liegt vor allem in höherem Speicherplatz, dem Auslesen aus der Distanz ohne direkten Sichtkontakt zum Lesegerät und den kryptografischen Fähigkeiten, die ein Kopieren des Funketiketts praktisch ausschliessen.

Foto: Wammes Waggel (https://commons.wikimedia.org/wiki/File:RFID-capsule.jpg)
https://creativecommons.org/licenses/by-sa/3.0/deed.en

Die Kehrseite der RFID-Technologie versetzt Datenschützer jedoch in helle Sorge: Durch die hohe Speicherkapazität der Chips können sowohl Gegenstände als auch Personen direkt identifiziert werden. So könnte die Position eines Menschen und dessen Interaktion mit Gegenständen rund um die Uhr durch eine grosse, verknüpfte Infrastruktur von Millionen Lesegeräten analysiert werden und ein nahezu gläserner Bürger entstehen. Da das Auslesen des Chips unbemerkt stattfinden kann, könnte ein umfassendes Verhaltensprofil von Personen ohne deren Wissen erstellt werden.

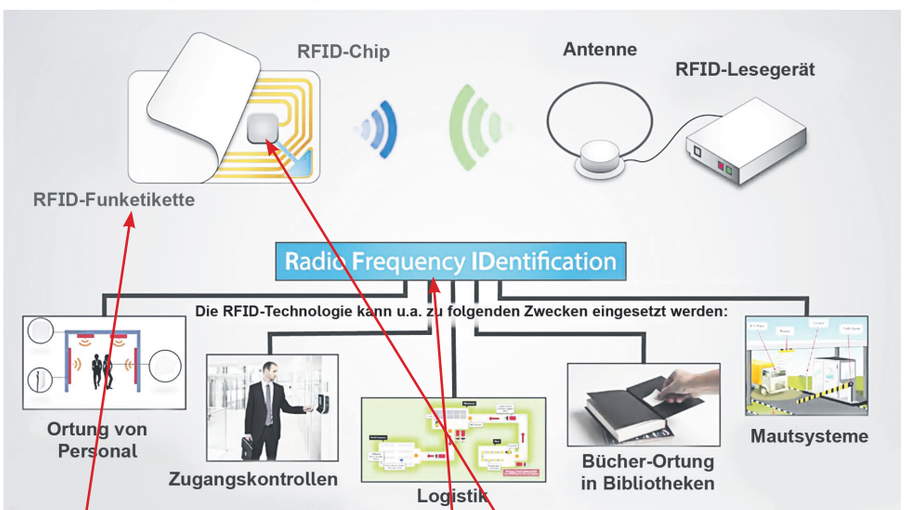
Zwar ist die RFID-Technologie seit Jahren in Industrie und Handel auf dem Vormarsch, doch die Schaffung einer riesigen Datenbank aller RFID-Lesegeräte wird höchstwahrscheinlich nicht von den Konzernen ausgehen, sondern in letzter Konsequenz von Regierungen, die diese Daten heute entweder schon von den Konzernen bekommen oder die Unternehmen früher oder später dazu verpflichten könnten, die Daten an sie weiterzuleiten. Ein Schritt in diese Richtung ist z.B. die weltweite Einführung von RFID-Ausweisen/Reisepässen, deren Daten man nur noch mit den Daten der Unternehmen verknüpfen müsste, um das vollständige Konsumverhalten eines Bürgers zu erfassen.

Mit dem allumfassenden Wissen über das Verhalten eines Individuums könnte auch die allumfassende Bestrafung von unerwünschtem Verhalten einhergehen, z.B. durch die Verknüpfung einer Schokoriegel-Verpackung auf einer Wiese mit dem Käufer und die Bestrafung des Käufers als Müllsünder. Es stellt sich die Frage, ob eine solche Zukunft ohne Geheimnisse wirklich wünschenswert ist.

Es ist zudem der Regierung vorbehalten, wen sie als «Verbrecher» kategorisiert und bestraft. Im Laufe der Geschichte wären dies nicht immer nur Schwerverbrecher, sondern genauso Regimekritiker. Was wären z.B. die Konsequenzen davon, wenn die Polizei in wenigen Sekunden die Identität hunderter Teilnehmer einer regimekritischen Demonstration ermitteln könnte? Je nach Gesetzeslage, könnte man die Anwesenheit auf der Demonstration in Windeseile digital bestrafen (durch Bussgelder, eine Einstufung als «Verfassungsfeind» uvm.). So könnte ein totalitärer Staat seine Bürger weitaus effektiver unterdrücken als zuvor.

Momentan wird uns der RFID-Chip unter der Haut noch als optional angeboten, doch möglicherweise könnte diese Freiwilligkeit sich eines Tages zum Zwang entwickeln. Der obligatorische RFID-Chip im Körper könnte den Ausbruch aus einem totalitären Überwachungssystem endgültig unmöglich machen.

Was ist eine RFID-Funketikette?

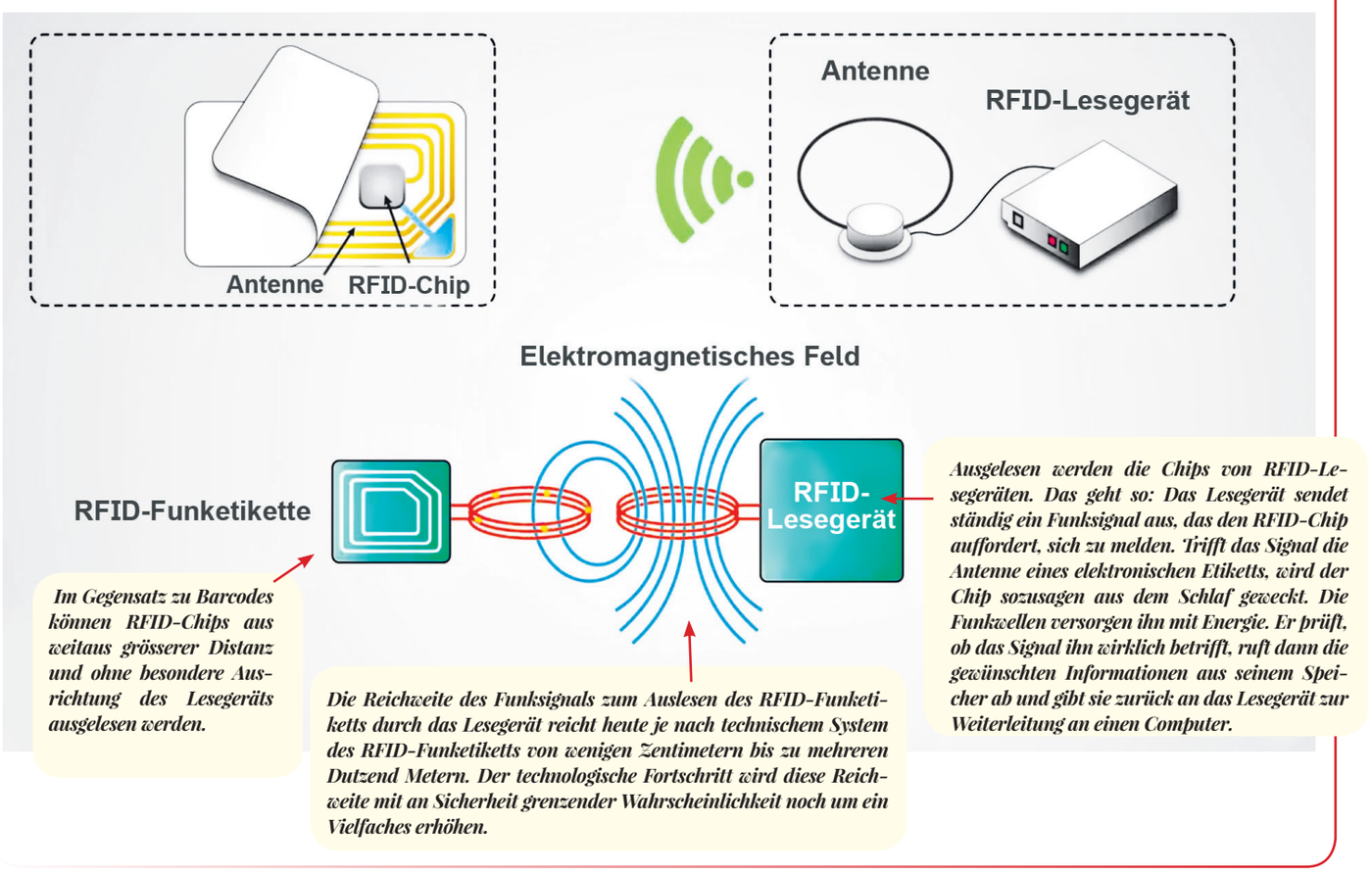


Drahtlose Funketiketten (englisch: RFID Tags) sind Datenträger, die eine Identifikationstechnik ähnlich dem altbekannten Barcode ermöglichen. Allerdings kann der heute in jedem Supermarkt benutzte EAN-Barcode maximal 13 Zeichen speichern. Das reicht gerade für die Angabe von Hersteller und Warenart. Es ist aber nicht genug, um beispielsweise in einer Leihbücherei die Betriebsdaten zu den Büchern aufzunehmen, also neben Titel und Autor etwa Inventarnummer, Anschaffungsdatum, Zahl der Ausleihungen oder den Standort in den Regalen. Büchereien in Wien und Stuttgart setzen daher RFID-Chips ein, die bis zu 10.000 Bit speichern. Das entspricht etwa einer Schreibmaschinenseite Text. Es ist jedoch abzusehen, dass die Speicherkapazität der Chips mit der technologischen Weiterentwicklung ansteigen wird. Der Vorteil von RFID-Tags liegt ganz generell darin, dass sich Dinge damit eindeutig identifizieren und wiederfinden lassen.

Laien sprechen selten von «Funketiketten» oder «RFID Tags». Sie haben lediglich vom «RFID-Chip» gehört. Damit beziehen sie sich auf den identischen Gegenstand: Der RFID-Chip ist das wichtigste Bauteil von elektronisch lesbaren Funketiketten. Auf ihm werden die Daten gespeichert.

RFID ist die Abkürzung für «Radio Frequency Identification» und bedeutet die Identifizierung von Dingen per Funk, also ohne sie zu berühren. Es geht darum, Daten kontaktlos aus einem Speicher auszulesen, hineinzuschreiben oder zu lös chen. Diese Daten identifizieren einen Gegenstand eindeutig und beschreiben seine Eigenschaften wie z.B. Typ, Herstelldatum oder Preis. Der Vorteil gegenüber dem Strichcode besteht bei RFID darin, dass dies über Funkwellen auch ohne direkte Sicht des Lesegeräts funktioniert.

Eine Zukunft ohne Geheimnisse?



Die Vorteile von RFID-Chips

Gegenüber dem optischen Auslesen eines Barcodes bietet die Verwendung von RFID-Funketiketten eine Reihe signifikanter Vorteile:

1. **Automatisierung:** Während Barcodes eine Sichtverbindung zum Lesegerät benötigen, die entweder manuell hergestellt bzw. auf Fliessbändern aufwändig durch mehrere Aufdrucke und/oder verschieden orientierte Lesegeräte sichergestellt werden muss, können Funketiketten prinzipiell ohne besondere Ausrichtung, d.h. auch «um die Ecke» bzw. «von hinten» gelesen werden.

Foto: Shutterstock/chombosan

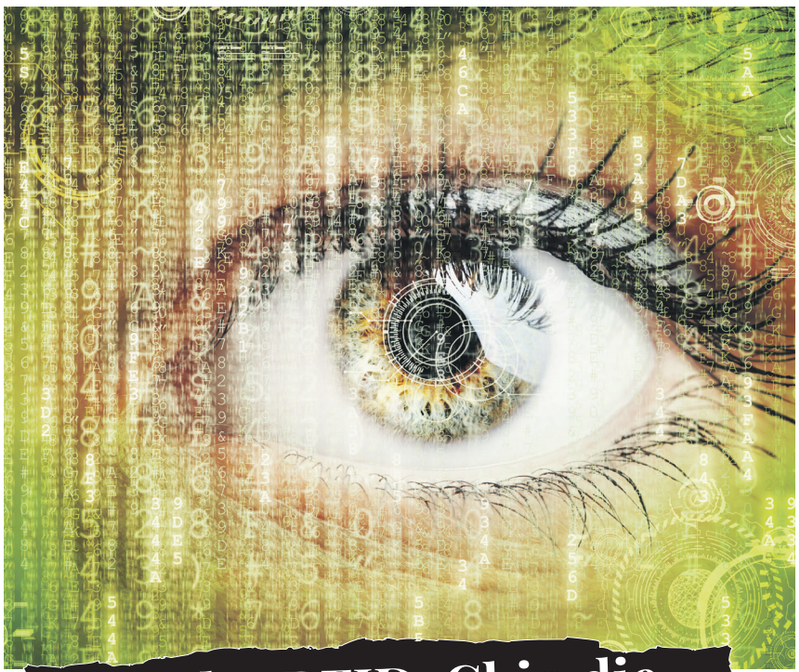
2. Identifizierung: Funketiketten ermöglichen es, mehr Informationen auf kleinerem Raum unterzubringen und können dadurch nicht nur eine Produktklasse identifizieren («Dies ist eine Packung Margarine»), sondern auch individuelle Seriennummern («Dies ist Margarinen- Packung #94810394»), die beispielsweise durch Verknüpfung mit einer Herstellerdatenbank weitere Detailinformationen verfügbar machen kann (z.B. «produziert am 11.6.2006 in Werk 4»).

3. Integration in das Produkt: Infolge der drahtlosen Kommunikation zwischen Lesegerät und Funketikett können Hersteller RFID-Funketiketten beinahe beliebig in ein Produkt integrieren. Mit der Hilfe von RFID können also, zumindest prinzipiell, Produkte und Gegenstände weitaus verlässlicher, einfacher und genauer identifiziert werden als mit traditionellen Barcodes.

4. Authentisierung: Darüber hinaus bietet RFID jedoch noch einen weiteren, entscheidenden Vorteil gegenüber Barcodes: Ausgestattet mit entsprechenden kryptografischen Fähigkeiten kann ein Kopieren eines Funketiketts praktisch ausgeschlossen werden. Während ein Barcode konstruktionsbedingt alle in ihm «enthaltene» Information für jegliche Lesegeräte gleichermassen zur Verfügung stellt, können im drahtlosen Kommunikationsprotokoll zwischen RFID-Funketikett und Leser aufwändige Identitätsprüfungsmechanismen integriert werden, die nicht nur unautorisierten Lesegeräten das Auslesen verbietet, sondern ebenfalls sicherstellen, dass ein auf dem Funketikett gespeichertes Geheimnis nicht direkt auslesbar ist, dessen Vorhandensein jedoch vom auslesenden Lesegerät zweifelsfrei überprüfbar ist. Ein populäres Beispiel für einen solchen Einsatz ist die in fast allen modernen Fahrzeugen integrierte Wegfahrsperre: Ein im Autoschlüssel integrierter RFID-Chip wird beim Betätigen der Zündung von einem integrierten Lesegerät ausgelesen und identifiziert den Schlüssel als ein Original. Ein weiterer Grund für die Verwendung von drahtlosen Funketiketten ist also ihr Einsatz zur verlässlichen Identifizierung: Der Authentisierung.

Diesem Umstand verdanken RFID-Tags ihre abseits aller Proteste bereits weit fortgeschrittene Verbreitung in Eintrittskarten (z.B. als drahtloser Skipass in vielen Skigebieten bzw. im Rahmen der WM 2006 in Millionen von Eintrittskarten), als drahtloses Zahlungsmittel (z.B. in vielen Betriebskantinen, aber auch im in den USA beliebten Exxon-Speedpass zum bargeldlosen Tanken) und nicht zuletzt im neuen biometrischen Reisepass. Gerade die letzten Beispiele zeigen bereits, dass RFID-Tags eine recht grosse Bandbreite an Anwendungsgebieten abdecken – vom fälschungssicheren Reisepass bis hin zu Coladosen und Rasierklingen – und dass die technischen Anforderungen an die jeweils eingesetzten Tags sehr unterschiedlich ausfallen können.

Foto: Shutterstock/Brian A. Jackson



Wie der RFID-Chip die Privatsphäre bedroht:

So vorteilhaft der Einsatz von RFID-Tags gegenüber dem konventionellen Barcode sein kann – erhöhter Automatisierungsgrad, genauere Identifikation, unauffällige Integration und sichere Authentisierung – so unvorteilhaft sind diese Aspekte, wenn es um den Schutz der Privatsphäre geht:

1. Automatisierung: Mitgeführte Funketiketten lassen sich ohne die Zuhilfenahme der jeweiligen Trägerperson auslesen, in vielen Fällen sogar ohne manuelle Justierung des Lesegerätes. Dies senkt die Kosten und erleichtert so das Durchführen von Datensammlungen erheblich.

2. Identifizierung: Eine verbesserte Identifizierung einzelner Gegenstände erhöht gleichfalls die Möglichkeiten zur eindeutigen Identifikation der diesen Gegenstand mitführenden Person. Dies ermöglicht weitaus genauere Kunden- bzw. Bürgerprofile.

3. Integration: Die drahtlose Kommunikation erlaubt nicht nur das unbemerkte Auslesen, sondern auch das unbemerkte Anbringen eines Funketiketts an (bzw. in) einen Gegenstand. So könnte die Tatsache, dass ein Auslesen eines Gegenstandes überhaupt möglich ist, leicht vor dessen Besitzer verborgen bleiben.

4. Authentisierung: Die obigen Punkte sind besonders kritisch beim Einsatz solcher Funketiketten in Gesundheits-, Sicherheits- und Zahlungssystemen, bei denen personenbezogene Daten eng mit einem RFID-Tag verknüpft bzw. direkt darauf gespeichert sind.

Diese vier Aspekte drahtloser Funketiketten bedrohen zwei Arten der individuellen Privatsphäre: Die ortsbasierte Privatsphäre (das Recht, seinen Standort geheim zu halten) und die informationelle Privatsphäre (das Recht, bestimmte Bereiche seines Lebens nicht offenzulegen).

Ortsbasierte Privatsphäre: Sobald ein von einer Person mitgeführter, mit Funketiketten ausgestatteter Gegenstand von einem Lesegerät identifiziert wird, kann auf den momentanen Aufenthaltsort dieser Person geschlossen werden. Dies funktioniert nicht nur mit eindeutiger Identifikation der Person: auch wenn lediglich Produktgruppen, z.B. ein bestimmtes Jeansmodell bzw. eine bestimmte Schuhmarke identifiziert werden, so können durch die spezifische Kombination dieser Gegenstände individuelle Personen identifiziert werden. Durch das Wissen um die Aufenthaltsorte persönlicher Gegenstände, z.B. dass der Wagen einer Person um eine bestimmte Zeit eine automatische Mautstation passiert hat, können andere leicht auf die Bewegungen ihrer Besitzer – und damit in den meisten Fällen auch auf deren Tätigkeiten – schliessen.

Informationelle Privatsphäre: Sobald die drahtlosen Funketiketten nicht nur zufällige Zahlenreihen darstellen, sondern Daten (z.B. eine Kundennummer oder eine Herstellerangabe) bzw. sobald sie über eine Datenbank mit Daten verknüpft werden können, wird über die Ortung hinaus auch die informationelle Privatsphäre der Person bedroht. Gleichermassen kritisch ist die Speicherung von personenbezogenen Daten direkt auf dem RFID-Funketikett, z.B. Ort und Datum des Kaufs eines Produkts. Einen besonderen Fall stellt das Auslesen von Produkt-Funketiketten dar, deren Mitführen nicht öffentlich bekannt ist. Hierunter fallen die oft zitierten Beispiele vom Auslesen der Unterwäschemarke einer Person, der Inhalt von Einkaufstaschen und das Ausspionieren von Einrichtungsgegenständen in einer Wohnung. In vielen Fällen kommt es dabei gar nicht darauf an, die Identität einer Person in Erfahrung zu bringen – es reicht zu wissen, dass diese Person einen Schwangerschaftstest in der Apotheke gekauft hat oder dass in diesem Haus modernste Unterhaltungselektronik steht.

Damit ist das Überwachungspotenzial von RFID-Chips nahezu allumfassend: Behörden oder Unternehmen könnten herausfinden, wo Sie gerade sind, welche Automarke Sie gerade fahren, welche Krankheit Sie plagt und ob Sie Arbeitslosengeld beziehen. Nahezu vollständige Profile Ihres Konsumverhaltens könnten erstellt und Ihre Position von auf der ganzen Welt verteilten RFID-Lesegeräten ermittelt werden. Da jedes einzelne Objekt durch seine individuelle Identifikation einem bestimmten Käufer zugeordnet werden könnte, wäre das Ausmass der Überwachung so umfassend, dass z.B. mit Funketiketten versehener Abfall zum Käufer zurückverfolgt werden könnte, um so Müllsünder, z.B. in öffentlichen Parks, zur Rechenschaft zu ziehen. Ebenso beunruhigend wirkt es, in welchem Ausmass mit RFID gekennzeichnete Gegenstände von smarten Umgebungen dazu verwendet werden könnten, gesellschaftlich erstrebenswertes Handeln zu erzwingen, wie beispielsweise Mülleimer, die keine Glasflaschen mehr akzeptieren oder Versicherungsprämien, die in Abhängigkeit vom gesunden oder ungesunden Kaufverhalten steigen oder fallen.

Quelle: RFID und die Zukunft der Privatsphäre, Marc Langheinrich, Inst. für Pervasive Computing, ETH Zürich

Foto: Shutterstock/a-image

Die totale Vernetzung jeder Person und jedes Gegenstandes durch RFID

RFID-Chips sind überall auf dem Vormarsch. Ob Sie Auto fahren (Funkschlüssel, Wegfahrsperre), als Waldarbeiter Bäume im Wald einsammeln, einen Skilift benutzen, ein Fussballspiel besuchen oder als Einzelhändlerin Ihre Joghurt-Becher drahtlos erfassen wollen - fast überall werden inzwischen Lösungen mit RFID angeboten. Und das oft zum Vorteil der Anwender, doch mit grossen Risiken und Kosten für das Personal, die Kundschaft oder die Bürger:

- Eintrittskarten / Tickets
- Einzelhandel
- Lagerhaltung
- Bahncard und Fahrkarten
- Ausweise und andere Identitätspapiere
- Sport
- Geldscheine
- Bücher
- Tierkennzeichnung
- Waldwirtschaft
- Wohnbereich

Diese Liste ist keineswegs vollständig und nicht alle der Anwendungen sind eine Gefahr für den Datenschutz oder unsere Bürger- und Freiheitsrechte, doch die Frage muss gestellt werden, wieweit wir es als Gesellschaft erlauben sollten, die RFID-Technologie in unser Leben eindringen zu lassen.

Erklärtes Ziel der RFID-Lobby ist es, in den kommenden Jahren alles, jede Steckdose, jede Hose, jeden Schuh und jeden Joghurtbecher mit RFID auszustatten. Und jedes Produkt, das mit RFID verkauft wird, ist ein Schritt in diese Richtung. Folgerichtig ist der Handel der wichtigste Partner bei der Einführung der Technologie. In verschiedenen Läden werden schon jetzt Bewegungsprofile von Kunden mit RFID erstellt oder es wird erfasst, ob Werbe-Displays, an denen jemand vorbei gegangen ist, direkten Einfluss auf das Kaufverhalten haben. Wenn die Chips mit dem Kunden den Laden verlassen, sind sie allerdings keineswegs Müll: Sie bleiben aktiv bzw. sie werden weiterhin ihre Daten preisgeben, sobald sie angefunkt werden, egal von wem. Noch ist das kein wirklich grosses Problem (zumindest nicht für die Privatsphäre), weil wir noch keine flächendeckende Infrastruktur von Lesegeräten haben. Sind die Chips aber erst im Umlauf, könnten die Lese-Antennen an jeder vorstellbaren Ecke nicht lange auf sich warten lassen. Und dann könnte bald jede Tanksäule wissen, welches Kaugummi wir in der Tasche haben und uns während des Tankens Spots von Konkurrenzprodukten vorspielen.

Sicher hat das Vorteile, z.B. treffsichere Empfehlungen beim Einkaufen oder die Ortung eines verlorenen Produktes. Doch dafür nimmt der Bürger in Kauf, dass seine Position und sein Verhalten im Falle der Vernetzung aller Daten vollständig erfasst werden können. Höchstwahrscheinlich werden es nicht die Konzerne sein, die gemeinsam ein grosses Bewegungs- und Verhaltensprofil jedes Menschen erstellen, sondern die Regierungen, welche die Daten der Konzerne entweder schon bekommen oder die Unternehmen früher oder später dazu verpflichten könnten, die Daten an die Regierungen weiterzuleiten. Zudem könnten die Daten des biometrischen RFID-Ausweises/Reisepasses, der in Deutschland schon 2005 eingeführt wurde, mit den Daten der Unternehmen verknüpft werden, womit die echte Identität einer Person in Kombination mit ihren Handlungen nicht mehr über Umwege, sondern direkt ermittelt werden könnte.

Quelle: digitalcourage.de, Wo gibt es RFID?

Die Einführung von RFID-Ausweispapieren

Man fürchte die Bundesregierung, auch wenn sie Geschenke bringt

Seit November 2005 enthalten die neuen elektronischen und mit biometrischen Merkmalen versehenen EU-Reisepässe (ePässe) in Deutschland einen RFID-Chip. RFID-Chips in Ausweisen sind für Überwachungs-Zwecke besonders effektiv, denn das indirekte Erfassen eines Menschen über die Gegenstände, die er bei sich trägt (Schuhe, Jacken, Kaugummipackungen) ist recht aufwendig. Schliesslich muss zur Zeit noch bei jedem erfassten Chip eine Rückfrage an mehrere Datenbanken gestellt werden: «Wer hat diese Schuhe damals wo mit welcher Kunden-/Kreditkarte gekauft?» Bei Ausweisen ist der Weg direkt: «Wem gehört dieses Ausweispapier?» Minimalforderung sollte also sein, dass die Daten auf dem Funkchip verschlüsselt werden und nur von «berechtigten Stellen», z.B. Grenzkontrollen, ausgewertet werden dürfen. Das ist aber nicht vorgesehen - und wer sollte auch sicherstellen, dass nicht trotzdem Unbefugte Zugriff auf die Daten erhalten?

Auf den ersten Blick erscheint es sinnvoll, dass z.B. die Polizei die Chips in den Ausweisen entschlüsseln könnte, was auf den zweiten Blick allerdings bedeutet, dass ein Lesegerät neben einer Demonstration innerhalb von Sekunden alle Teilnehmer/innen erfassen kann, ohne dass diese das überhaupt merken. So gäbe es möglicherweise in naher Zukunft keine Möglichkeit mehr, sich als gesuchte Person in Gebieten voller RFID-Lesegeräte der Strafverfolgungsbehörden zu bewegen. Die Polizei müsste nicht mehr mühsam nach Kriminellen suchen, die Lesegeräte würden deren Position früher oder später verraten. So würde die Möglichkeit «unterzutauchen» und sich vor den Behörden zu verstecken, nahezu unmöglich gemacht.

Der gesetzestreue Bürger mag damit kein Problem haben und sich die Frage stellen: «Was spricht dagegen, wenn die Behörden Verbrecher leichter aufspüren können?» Damit mag er zum Teil Recht haben, doch die Schattenseiten dieser Entwicklung blendet er aus: Erstens spricht wenig dafür, dass Regierungen nur die Daten von Verbrechern auslesen und analysieren würden. Auch jedes Detail im Leben des bravsten aller braven Spiessbürger könnte dem Staat in Zukunft jederzeit zur Verfügung stehen. Zweitens ist es der Regierung vorbehalten, wen sie als «Verbrecher» kategorisiert und das waren im Laufe der Geschichte nicht immer nur Mörder, Vergewaltiger und Diebe, sondern ebenso z.B. Friedensaktivisten oder Gegner der herrschenden Partei. Was wären z.B. die Konsequenzen davon, wenn die Polizei in wenigen Sekunden die Identität hunderter Teilnehmer einer regimekritischen Demonstration ermitteln könnte? Je nach Gesetzeslage könnte man die Anwesenheit auf der Demonstration in Windeseile digital bestrafen (durch Bussgelder, eine Einstufung als «Verfassungsfeind» uvm.). Die Polizei erspart sich damit ausserdem die anstrengende und zeitintensive Ausweiskontrolle von möglicherweise aufmüpfigen Bürgern.

Quelle: digitalcourage.de, Wo gibt es RFID?

Datenschützer warnen vor RFID-Chips in Kleidung

Sie gehen in die Stadt und kaufen einen Anzug. Beim Betreten des nächsten Geschäfts spricht Sie ein Verkäufer an und teilt Ihnen mit, dass die zu Ihrem neuen Anzug passenden Krawatten momentan knallhart reduziert sind. Da bleibt Ihnen die Spucke weg: Denn Sie haben weder danach gefragt noch Einblick in Ihre Einkaufstasche gewährt.

Der Verkäufer ist trotzdem bestens darüber informiert, was sich in Ihrer Einkaufstüte befindet. Er weiss sogar, wo Sie die Waren wann gekauft und was Sie dafür bezahlt haben. Verraten hat Sie der RFID-Chip, der in Ihre Einkäufe eingenäht ist und dessen zunehmende Anwendung Datenschützer auf die Palme bringt. Informationen zum Kleidungsstück lassen sich über eine Online-Datenbankabfrage blitzschnell ermitteln.

Immer mehr Einzelhandelsketten für Kleidung, darunter Peuterey, Lemmi Fashion, Levi's, Gerry Weber und s'Oliver, setzen bereits auf RFID-Chips. Die Mitglieder des Bielefelder Datenschutzvereins FoeBuD (FoeBuD ist die Abkürzung für «Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.») setzen sich gegen den Einsatz dieser Technik in Kleidung zur Wehr und machen Bürger durch Aktionen vor Geschäften darauf aufmerksam.

Die RFID-Chips sind so klein, dass sie unauffällig ohne das Wissen des Käufers in den Waschzettel eingenäht werden können.
Foto: shutterstock/Nataliya Turpitko

Die Bedenken gehen über individuelle Einkaufstipps für identifizierte Kunden weit hinaus: Menschen können über Funkchips in Kleidung heimlich geortet und Bewegungsprofile erstellt werden. Tatsächlich haben die meisten Kunden keine Idee davon, dass ihre Kleidung Signale aussenden könnte.

Die Antenne, über die der Chip auch den Strom bezieht, ist so winzig, dass sie problemlos in einen Waschzettel eingenäht werden kann. Chip und Antenne sind so robust, dass sie Waschgänge überstehen und jahrelang ihre Seriennummer an RFID-Lesegeräte in der Nähe senden können.

Die Risiken, auf die FoeBuD hinweist, sind real. Besonders bedenklich ist, dass einige Hersteller, z.B. Peuterey, ihre Kunden gar nicht oder nicht ausreichend über eingenähte Funkchips informieren und deren Entfernung sogar verhindern wollen. Computer Bild machte den Test in einer Gerry-Weber-Filiale. Hier sind RFID-Chips in den Waschzettel eingenäht. Anders als andere Hersteller empfiehlt Gerry Weber, den Chip nach dem Kauf herauszuschneiden. Doch warum sollte der Chip nicht bereits nach dem Kauf von einem Mitarbeiter entfernt werden? Computer Bild schreibt: Alle Textilanbieter sollten ihre Kunden über RFID-Chips informieren und RFID-Sender gleich an der Kasse ungefragt entfernen.

Quelle: welt.de, Datenschützer warnen vor RFID-Chips in Kleidung, 20.02.2012

Elektronische Gesundheitskarte – ein weiterer Schritt hin zum Überwachungsstaat

Im Dezember 2015 hat der Bundestag das «Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen» (kurz: e-health-Gesetz) verabschiedet. Damit wurde die neue elektronische Gesundheitskarte, kurz: eGK, mit dem RFID-Chip für alle Kassenpatienten gesetzlich eingeführt. Während die Befürworter in Politik und Wirtschaft in der eGK und Zentralspeicherung von Gesundheitsdaten kein Problem sehen, warnen IT-Fachleute, Ärzteverbände und Patientenvertretungen davor, sich auf die eGK und die dahinter stehende Zentralspeicherung von Gesundheitsdaten einzulassen. Diese ist aber fest eingeplant, denn das Projekt rechnet sich für die Industrie nur, wenn alle Karteninhaber die «freiwillige» Funktion der Gesundheitsdatenspeicherung nutzen. Daher wird mächtig Druck ausgeübt: Wer an der Datensicherheit zweifelt, sein Bild nicht freigibt, die Karte nicht nutzt oder Widerspruch einlegt, wird schikaniert. Patienten werden nicht behandelt, müssen versicherte Behandlungen dennoch privat bezahlen oder die Krankenkassen fordern dazu auf, die Krankenkasse zu wechseln. Auch Ärzte werden – laut e-health-Gesetz – mit Geld und Fristen sanktioniert. Zeigen sich darin nicht die Ansätze eines Überwachungsstaates?

Quelle: Stimme und Gegenstimme, 06/2017

"... haben Sie ein Problem mit Furunkelbildung im Gesäßbereich!"

Von der Freiwilligkeit zum Zwang? Könnte eines Tages jedem Menschen ein Chip implantiert werden?

Momentan wird uns der RFID-Chip unter der Haut immer noch als optional angeboten: Allmählich steigt die Zahl der Menschen, die sich freiwillig einen Chip implantieren lassen. Möglicherweise soll eine kritische Masse an Menschen erreicht werden, die ihren Körper bereitwillig dem neuen Überwachungswerkzeug zur Verfügung stellen, um daraufhin auch alle anderen zum RFID-Chip unter der Haut zu zwingen.

Bereits 2004 wurde 168 Mitarbeitern im Nationalen Informationszentrum in Mexiko ein RFID-Chip unter die Haut gepflanzt, der nicht entfernbar (!) sein soll. Einerseits erhält der Mitarbeiter mit dem RFID-Chip Zutritt zum Hochsicherheitsareal, andererseits kann er aber auch auf Schritt und Tritt überwacht werden. Das RFID-Chip-Implantat erlaubt es, die Mitarbeiter jederzeit und überall zu orten, wo Lesegeräte in der Nähe und gegebenenfalls unauffällig getarnt sind.

Diese Lesegeräte können auch mobil sein und über GPS verfügen, so dass Ort und Zeit der Kontaktaufnahme mit dem RFID-Chip gespeichert werden können. Aus Angst vor Entführungen liessen deshalb auch wohlhabende Eltern aus Südamerika ihre Kinder mit RFID-Chips ausstatten. Bei Straftätern werden die Implantate als Ersatz für elektronische Fussfesseln angewendet, um - in Kombination mit einem Sender - ihren Aufenthaltsort zu überwachen. Im medizinischen Bereich sind RFID-Chip-Implantate ebenfalls im Einsatz, z.B. bei Demenzkranken. Auch der Jugend wird der Chip schmackhaft gemacht: So erhalten z.B. Gäste im Baja Beach Club in Barcelona und in der Bar Soba in Glasgow VIP-Zugang, wenn sie sich von einem Disco-Arzt «chippen» lassen.

Foto: shutterstock/M-SUR

In Schweden haben sich laut Medienberichten z. B. über 300 Büroangestellte freiwillig einen Chip implantieren lassen, um sich u.a. bei Türen und Kopiergeräten identifizieren lassen zu können. Laut einem Artikel des Schweizer Migros-Magazins vom März 2017 ergab eine globale Studie, «dass 70 Prozent der befragten Teenager so ein Implantat möchten, falls es ihre digitale Freiheit im Leben steigert.»

Kirstie Ball, Soziologin an der Open University Business School in Milton Keynes (England) sagte dazu: «Der Keim für die Technologie ist gelegt. Sie wird sich in nächster Zeit ausbreiten»

Quellen: kla.tv, Kommt die Totalüberwachung per implantierten RFID-Chip in Mode?, 17.04.2016
kla.tv, Chip-Implantatentwicklung birgt gewaltiges Missbrauchspotential in sich, 17.06.2017

Läuft bald nichts mehr ohne RFID-Chip?

Am 01.8.2017 wurde bei Mitarbeitern der Firma «Three Square Market» (32M) zwischen Daumen und Zeigefinger auf freiwilliger Basis ein RFID-Chip implantiert. Damit ist 32M eine der ersten US-Firmen, die ihre Mitarbeiter chippt. So kann man an 2000 Standorten über den Chip im firmeninternen Kiosk einkaufen, Türen öffnen und Kopierer aktivieren. Auch medizinische Gesundheitsinformationen werden dort gespeichert. Ideengeber war laut 32M die schwedische Firma BioHax, die in Helsinki ihre Belegschaft bereits gechippt hat. Todd Westby, der oberste Chef dieser Firma, sagte: «Eines Tages wird diese Technik standardisiert sein und Ihnen ermöglichen, [den Chip] als Reisepass und Fahrausweis sowie für alle Einkaufsmöglichkeiten zu nutzen.» Dieser wird zwar auf freiwilliger Basis implantiert, aber wie kommen langfristig Mitarbeiter ohne Chip bei 32M zurecht?

Quellen: Stimme und Gegenstimme, 38/2017
heise.de, Chip-Implantat zur Identifikation: Firma will Mitarbeitern Chips einsetzen, 24.07.2017

Foto: Paul Hughes (https://commons.wikimedia.org/wiki/File:Dr_Mark_Gasson_has_an_RFID_microchip_implanted_in_his_left_hand_by_a_surgeon_(March_16_2009).jpg) https://creativecommons.org/licenses/by-sa/4.0/deed.en

Foto: Lucélia Ribeiro (https://commons.wikimedia.org/wiki/File:Children_at_school_(8720604364).jpg) https://creativecommons.org/licenses/by-sa/2.0/deed.en

Der Köder? RFID-Chips zur Sicherheit von Kindern

Am 08.12.2016 verabschiedete das amerikanische Repräsentantenhaus ein Gesetz, das dem Generalstaatsanwalt in Zusammenarbeit mit dem Gesundheitsminister erlaubt, die Standortverfolgung von Zielpersonen voranzutreiben. Mit Hilfe von RFID-Lesegeräten sollen Personen mit implantierten RFID-Chips gefunden werden. Obwohl dieses Gesetz angibt, lediglich Demenzkranke oder entwicklungsgestörte Kinder, die sich aus ihrer sicheren Umgebung entfernt haben, wiederfinden zu wollen, könnte sich dies als «Trojanisches Pferd» erweisen. So sagte der Abgeordnete Louis Gomert in seiner Rede im Repräsentantenhaus, dass diese Initiative noble Absichten haben möge, aber solche Programme zum Schutz und zur Sicherheit der Bevölkerung würden häufig zu festen staatlichen Überwachungseinrichtungen entarten, die die Freiheit des amerikanischen Volkes einschränken. Wenn erst einmal ein Netz von RFID-Lesegeräten entstanden ist, wird es nicht mehr schwierig sein, dieses Überwachungsprogramm beliebig auszudehnen.

Quelle: Stimme und Gegenstimme, 04/2017

Kindersendung wirbt für Implantierung

Seit einigen Jahren ist zu beobachten, wie unsere Leitmedien augenscheinlich im Gleichklang für das Implantieren des RFID-Chips in den menschlichen Körper werben. Hierbei werden die scheinbaren Vorzüge dieser Technik betont. In Fernsehreportagen werden Einsatzbereiche vorgestellt, in denen der Funkchip sinnvoll zu sein scheint, wie z.B. als Patientenarmband, im Parkticket, zur Haustieridentifikation, in Fahrscheinen, als Zahlungsmittel an der Bar oder Fitnesszentren sowie in der Kleidungs- und Lebensmittellogistik. Sogar Journalisten lassen sich öffentlichkeitswirksam vor laufender Kamera einen RFID-Chip implantieren, offensichtlich um bei den Zuschauern Hemmschwellen abzubauen.

Zielgruppe dieser medialen Meinungsmache sind seit Neustem auch die Kinder. So wirbt der Fernsehsender KiKA in seiner Sendereihe «Erde an Zukunft» für die transhumane Technologie. Das meint eine Technologie, in der menschliche Grenzen überwunden werden sollen.

In der Sendung «Cyborg! halb Mensch - halb Maschine» vom 5.3.2016 beschreibt ein kleiner Junge, wie toll es doch wäre, durch Verschmelzung von Mensch und Technologie, was ja genau einen «Cyborg» ausmacht, mit übermenschlichen Superkräften ausgestattet zu werden. Diese Zukunftsaussichten wertet der Moderator der Sendung Felix Seibert-Daiker als ziemlich cool. Er erklärt den Kindern anhand verschiedener Beispiele, wie auch Menschen mit einer Einschränkung wie z.B. Gehörlosigkeit, Farbenblindheit oder einer Gehbehinderung, durch Verschmelzung mit technischen Hilfsgeräten zu einem Cyborg-Menschen werden und dadurch ihre Einschränkungen ausgleichen können.

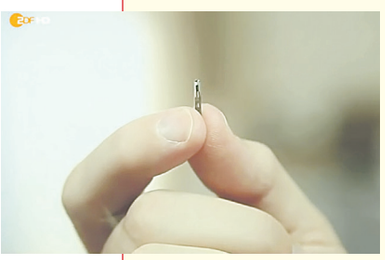
Aber nicht nur aus medizinischen Gründen scheint laut dem Fernsehsender KiKA die Implantierung eines RFID-Chip sinnvoll zu sein. Den Kindern wird nämlich nahegelegt, dass es sich hierbei um einen «Trend» handle: Ähnlich wie bei einem Tattoo oder Piercing könnten sie sich für ein RFID- Implantat entschliessen. Dadurch könnten sie sich in einen «Spass-Cyborg» verwandeln, der verschlossene Türen öffnen oder mit dem Handy wichtige Daten übertragen kann. Hierfür müsse man lediglich 18 Jahre alt sein. Für Jüngere brauche es nur die Einverständniserklärung der Eltern, so Moderator Felix.

Die Freunde Angelo und Rin bezeichnen sich in der KIKA-Dokumentation als «Spass-Cyborgs», die sich deshalb Funkchips unter die Haut implantieren liessen. So werden bereits Kleinkinder für die Verschmelzung von Mensch und Maschine sensibilisiert. Der KIKA-Beitrag verzichtete darauf, auf die vielen Schattenseiten des Chips im Körper einzugehen.

ZDF macht Zuschauern den RFID-Chip schmackhaft

In einem äusserst einseitigen Beitrag hat das ZDF im Februar 2016 dafür geworben, dass die Zukunft des Zahlungsverkehrs bei implantierbaren RFID-Chips liege. In Schweden sei bereits ein Pilotprojekt zur bargeldlosen Bezahlung über solche RFID-Chips im Einsatz, schwärmte der Moderator Claus Kleber in der betreffenden Sendung und liess einen Software-Entwickler unwidersprochen Werbung für die angebliche Sicherheit der RFID-Technologie machen. Unter anderem behauptete dieser Folgendes:

«Wenn man mit Leuten darüber redet, hört man immer wieder, die Regierung könne dann ja sehen, wo man sich befinde, dass man seine persönliche Unabhängigkeit verliere usw. Das ist aber nicht der Fall, denn diese Chips senden keine Signale aus, man braucht ein Lesegerät damit sie funktionieren, sie sind passiv.»



Software-Experten widersprechen solchen Behauptungen vehement. Sollte die Bezahlung per Chip eines Tages tatsächlich zum Standard werden, dann wäre der Standort jedes gechippten Bürgers bei jeder getätigten Bezahlung gerade durch das verwendete Lesegerät und dessen potenzielle Vernetzung mit allen anderen Lesesystemen sofort nachvollziehbar. Dadurch liessen sich nicht nur für Geheimdienste, sondern auch für professionelle Hacker und Verbrecher jeder Art, mit einfachsten Mitteln präzise Verhaltensprofile erstellen. Es würde dadurch völlig transparent werden, wer wann und wo einkauft, essen geht, das Kino besucht oder öffentliche Verkehrsmittel nutzt. Dies wäre die Geburt des absolut gläsernen Bürgers.

Quelle: kla.tv, Drohende Bargeldabschaffung: ZDF wirbt für die Totalüberwachung per RFID-Chip, 06.03.2016

von Funkchips

Auf die Frage, wie weit diese Technologie in der Zukunft reichen wird, gibt der personifizierte Computer namens Lisa eine sehr aufschlussreiche Antwort:

«Mein lieber Felix, die Zukunft wird perfekt. Mensch und Maschine wachsen immer mehr zusammen. Geht einmal etwas kaputt, vielleicht ein Organ oder ein Knochen, ist das überhaupt kein Problem. Wie in der Autowerkstatt gibt es dann einfach ein Ersatzorgan, natürlich ein technisches. Selbst Emotionen werden mittels Sensoren und Minicomputer reguliert. Keine unkontrollierten Wutausbrüche mehr und alles ist fein säuberlich programmiert […] Bald wird man zwischen Mensch und Maschine nicht mehr unterscheiden können, wir beide werden einfach eins. […] Extrasensoren wird es geben und die passen auf dich auf, die kontrollieren, ob alles in deinem Körper rund läuft. Selbst kleine geistige Schwächen können wir ausgleichen. Dafür gibt es dann Mega-Hochleistungsprozessoren im Kopf.»

Stopp, was wurde da umworben? Emotionen werden mittels Sensoren und Minicomputer reguliert, Extrasensoren wird es geben, die auf dich aufpassen, Mega-Hochleistungsprozessoren im Kopf?

Genau vor dieser Entwicklung warnen doch Kritiker bereits seit längerer Zeit. Denn ein integrierter Sender im menschlichen Organismus hat wegen seiner tumorfördernden Eigenschaften nicht nur aus medizinischer Sicht sehr gefährliche Auswirkungen. Auf dieses Risiko der elektronischen Versklavung wurde in der Kinderreportage aber in gar keiner Weise hingewiesen.

Warum aber wird dennoch von den Leitmedien mit solch einer Intensität daran gearbeitet, der Bevölkerung und nun sogar auch den Kindern die Verwendung des RFID-Chips derartig schmackhaft zu machen?

Quelle: kla.tv, Kindersendung wirbt für Implantierung von Funkchips, 13.04.2016

Wird uns die Digitalisierung mit dem Argument des Komforts nur schmackhaft gemacht? Und verbirgt sich hinter den Versprechungen in Wahrheit ein Albtraum aus minimalem Lebensraum, minimaler Souveränität und maximaler Versklavung wie in George Orwells 1984? Der implantierte RFID-Chip wäre ein entscheidendes Werkzeug, um Big Brother die Gefangenschaft seiner Untertanen zu garantieren.

Kein Entfernen und kein Entkommen: Die beunruhigendste aller RFID-Dystopien

Wir bewegen uns zwar sowieso schon auf eine Welt zu, in der jede Handlung digital erfasst werden könnte und in der jede Person, die sich der Digitalisierung verschliesst, keine Möglichkeit mehr hätte, am kommerziellen und sozialen Leben teilzunehmen. Individuen, die ihre Position und ihre Daten nicht mit anderen teilen wollen, hätten in einer vollkommen digitalisierten Welt allerdings immer noch die Möglichkeit «unterzutauchen» und sich z.B. in der Natur selbst zu versorgen. Sicher keine sehr angenehme Perspektive, aber immerhin ein möglicher Ausweg aus dem weltweiten Überwachungsnetz. Denn nur weil uns die Digitalisierung mit wachsendem Komfort schmackhaft gemacht wird, bedeutet dies nicht, dass sich diese Versprechungen erfüllen müssen. Genauso könnten wir schmerzhaft aus dem angenehmen Traum der Welt ohne Arbeit gerissen werden, um in einem Orwell`schen Albtraum der digitalen Versklavung zu erwachen. In diesem Fall wäre eine Existenz abseits der «Zivilisation» möglicherweise die bessere von zwei schlechten Optionen. Zumindest könnte man so der digitalen Knechtschaft entgehen.

In dieser brutalen Dystopie wäre eine Möglichkeit, um den Ausbruch aus der «Zivilisation» endgültig zu verhindern, der Zwang zur Implantierung eines RFID-Chips, der ausserdem nicht entfernt werden könnte. So könnte man den Standort jeder Person jederzeit ermitteln. Die notwendige Technologie, um die Entfernung des RFID-Chips zu verhindern, existiert bereits. Wer probiert, seinen Chip zu entfernen, könnte z.B. einfach getötet werden: Die Augsburger Zeitung titelte basierend auf einer DPA-Meldung: «Tötungs-Chip beschäftigt deutsches Patentamt». Es wurde berichtet, dass ein Patent für einen implantierbaren Chip zur Überwachung und Tötung von Menschen eingereicht wurde.

Der Antragsteller hatte einen Chip entwickelt, der über eine sogenannte «Strafkammer» mit Gift verfüge. Das hochwirksame Gift sei «sicher eingekapselt, ausser wenn wir diese Person aus Sicherheitsgründen eliminieren wollen», heisst es in der Patentschrift. Laut Augsburger Zeitung hat das Patentamt aber den Antrag abgelehnt. Die Frage stellt sich, ob Rüstungskonzerne oder Geheimdienste, wenn sie im Besitz solch eines Tötungschips wären, überhaupt beim Patentamt vorstellig würden.

Quellen: macht-steuert-wissen.de, RFID-Chip für jeden – was steckt wirklich dahinter, 27.11.2017
augsburger-allgemeine.de, Chip für Überwachung und Tötung von Menschen, 08.05.2009

Bargeldverbot

- Gegen den klaren Mehrheitswillen der Bevölkerung treiben Banken und Politik die allmähliche Abschaffung von Bargeldzahlungen voran, angeblich um Kriminalität zu bekämpfen.
- Sollte das Bargeld tatsächlich eines Tages verschwinden, würde jeder einzelne Zahlungsvorgang überwachbar. Und da fast alles im Leben Geld kostet, wäre unser Leben ohne Bargeld künftig wie ein offenes Buch.
- Die Überwachung ist beim Gegenstand Bargeldverbot jedoch noch nicht einmal das eigentliche Thema: Das ausschliesslich elektronische Zahlungssystem wäre der Einstieg in die totale Sklaverei, denn mit einem Mausklick könnte der Staat oder die Bank jedem «den Geldhahn» zudrehen. Man würde sofort auf den Knien herumrutschen, nur um wieder zahlen zu können.

Angriff auf das Bargeld

«In zehn Jahren wird es kein Bargeld mehr geben.»

John Cryan, Vorstandsvorsitzender der Deutschen Bank 2016 in Davos

Stockholm, 5.15 Uhr. Der Morgen graut bereits, als über dem Stadtteil Västberga plötzlich Hubschrauberlärm zu hören ist. Über einem flachen, mehrstöckigen Gebäude zeichnet sich die Silhouette eines Helikopters ab. Plötzlich sind dunkle Gestalten zu sehen, die in Windeseile auf dem Dach abgesetzt werden. Wenig später sind mehrere Schüsse oder Explosionen zu hören. Es dauert etwa 15 bis 20 Minuten, bis der Hubschrauber die Dunkeltruppe wieder an Bord genommen hat – einschliesslich mehrerer grosser Säcke. Kurz darauf verschwindet er in der Morgendämmerung. Dies geschah am 23. September 2009. Damals raubte ein Kommando aus professionellen Kriminellen ein Gelddepot im Stockholmer Süden aus. Die Täter drangen über das Dach in das Gebäude der Stockholmer Geldfirma G4S ein, bahnten sich mit Trennschleifern und Sprengstoff einen Weg durch Gitter und Tresortüren und verschwanden 20 Minuten später mit 39 Millionen Kronen (4,1 Mio. Euro) im Gepäck im Morgenhimmel. Und dabei könnte man es eigentlich auch bewenden lassen, wenn sich seitdem nicht seltsame Dinge in Schweden und anderen Ländern der Europäischen Union tun würden.

Wer sind die echten Kriminellen?

2010, ein Jahr später, begann man die Dimension des Ganzen zu begreifen. Seit dem Raub ist Bargeld in Schweden nämlich des Teufels – in etwa so wie Waffen nach einem Amoklauf. Der Hubschrauber-Überfall in Stockholm diente als Startschuss für eine breit angelegte Kampagne gegen das Bargeld an sich: Bargeld, so lautet plötzlich der Tenor in Schweden, ist dunkel, böse, archaisch und einfach von Natur aus kriminell. Wer es besitzt, führt nichts Gutes im Schilde – genau so wie der Besitzer einer Waffe. Ohne Bargeld gäbe es kein Schwarzgeld und keine Schwarzarbeit, keine Steuerhinterziehung und natürlich auch keine Raubüberfälle mehr, lautet die Rechnung. Zu Weihnachten 2009 fand es die Polizeipräsidentin von Stockholm, Carin Götblad, besonders originell, einem fahrenden Weihnachtsbaumhändler zur Bezahlung ostentativ ihre Kreditkarte hinzuhalten. «Bargeld ist das Blut in den Adern der Kriminalität», meinte sie dazu.

Das ist natürlich Blödsinn – denn die grosse Kriminalität hat mit Bargeld überhaupt nichts zu tun, wie die jüngste Finanzkrise beweist. Ganz einfach deshalb, weil sich die wirklich grossen Summen nicht in bar transportieren und verschieben lassen. Die kriminellen Spekulationen, die zur Finanzkrise führten, wurden nicht in bar abgewickelt. Die grosse Finanzkriminalität hat weder etwas mit Portemonnaies noch mit Geldumschlägen, Geldkoffern oder Hubschraubern zu tun. Die wirklichen Schiebereien und Betrügereien, bei denen es um Milliarden geht, lassen sich mit Bargeld schlicht nicht abwickeln. Dazu ist es viel zu schwer und voluminös.

Jede Menge Ungereimtheiten

Der Überfall in Stockholm fiel demgegenüber geradezu in die Rubrik Kleinkriminalität: eine aussterbende Spezies von Kriminellen, die Leben, Gesundheit und Freiheit aufs Spiel setzen, um pro Nase ein paar hunderttausend Euro zu ergattern. Oder in die Kategorie «symbolische Inszenierung». Denn einige kleine Ungereimtheiten sprechen dafür, dass es sich tatsächlich nicht in erster Linie um einen Angriff auf ein Gelddepot, sondern auf das Bargeld an sich handelte.

Unter dem Strich ging es bei dem Stockholmer Raubüberfall am 23. September 2009 also nicht nur um einen Angriff auf ein grosses Bargelddepot. Es handelte sich auch um einen Angriff auf das Bargeld an sich. Zumindest wurde der Überfall

Foto: Lotus Head from Johannesburg, Gauteng, South Africa (https://commons.wikimedia.org/wiki/File:Credit-cards.jpg) https://creativecommons.org/licenses/by-sa/3.0/deed.en

Payback-Punkte – ein weiterer Baustein zur Steuerung der Bevölkerung

Angefangen hat es mit Rabattmarken bei Einkaufsläden, die gesammelt und, wie Briefmarken in ein Rabattheft eingeklebt, an der Kasse als Bargeld ausgezahlt wurden. Payback-Punkte funktionieren ähnlich? Falsch gedacht! Hier werden nämlich personenbezogene Daten über unsere Einkaufsgewohnheiten an ein kommerzielles Unternehmen verkauft. Solche Daten sind nicht nur für den Einzelhandel interessant, sondern werden auch durch Datenhändler wie Acxiom, Datalogix (Oracle) Epsilon oder Experian jährlich international für mehrere Mrd. Dollar gehandelt. Allein die US-amerikanische Firma Acxiom sammelt und analysiert auf 23.000 Servern mehr als 50 Milliarden Datentransaktionen pro Jahr; 96% aller US-Haushalte sind dort bereits erfasst.

Quelle: Stimme und Gegenstimme 16/17

Wird die Bevölkerung bewusst getäuscht?

Foto: shutterstock/nhungboon

Die Nutzung des Bargelds einzuschränken bzw. Bargeld abzuschaffen, wird in der Regel mit dem Kampf gegen Kriminalität, Korruption und Terrorismus begründet. Eine Studie der Deutschen Bank kommt jedoch zu einem gegenteiligen Ergebnis: Illegale Geschäfte und Terrorfinanzierung sind auch ohne Bargeld kaum zu stoppen. Länder wie z.B. Schweden, in denen der bargeldlose Zahlungsverkehr sehr fortgeschritten ist, weisen eine klare Verlagerung zur virtuellen Kriminalität (z.B. Kartenbetrugsdelikte) mit in der Regel deutlich höheren Schadensbeträgen auf. Damit erweisen sich die Argumente, mit denen eine Einschränkung bzw. Abschaffung von Bargeld gerechtfertigt wird, als unseriös.

Quellen: Stimme und Gegenstimme 01/2018
bundesbank.de, Die Zukunft des Bargelds, 07.03.2017

in einen solchen Angriff umgewandelt. Dabei mag es manche überraschen, dass das Recht auf Bargeld ein wichtiges Menschenrecht ist. Ein Menschenrecht, mit dem die meisten anderen Menschenrechte stehen oder fallen: Menschenwürde, Privatsphäre, persönliche Freiheit, Recht auf Eigentum usw. Und das Interessante ist, dass in der gesamten Menschheitsgeschichte noch nie jemand – kein Pol Pot, kein Josef Stalin und kein Adolf Hitler – auf die Idee gekommen ist, das Recht auf Bargeld abzuschaffen. Seit Beginn der Zivilisation war es immer und überall möglich, bar zu zahlen, sei es mit Gold- und Silber- oder Nickelmünzen, sei es mit Papiergeld oder Nuggets oder mit welchen Zahlungsmitteln auch immer. In der DDR genauso wie im Dritten Reich, unter der argentinischen Militärjunta ebenso wie im Stalinismus. Obwohl Bargeld von Haus aus antichristisch ist, zu Deutsch: herrschaftsfeindlich, konnte man überall unbeobachtet kaufen und verkaufen oder sein Geld für harte Zeiten im Sparstrumpf horten.

Dass ein Volk ohne Bargeld umgekehrt ein für alle Mal «erledigt» wäre, liegt auf der Hand. Denn sobald der Geldverkehr ausschliesslich unbar über Konten abgewickelt wird, lässt sich jede menschliche Regung bis ins Detail zurückverfolgen. Und nicht nur das: Mit einem weiteren Mausklick kann der Staat oder die Bank auch jedem «den Geldhahn zudrehen»: Der Mensch wird dann buchstäblich hilflos wie ein kleines Baby, und ihm droht die schlimmste Form von Unfreiheit in der menschlichen Geschichte.

Foto: 4028mdk09 (https://commons.wikimedia.org/wiki/File:International_Geldautomat_Commerzbank.JPG) https://creativecommons.org/licenses/by-sa/3.0/deed.en

Teures Bargeld soll zu bargeldloser Gesellschaft führen

Die Sparkassen Deutschlands hatten sich vor 20 Jahren das Ziel gesetzt, ihren Kunden innerhalb des eigenen Sparkassen-Netzes die gebührenfreie Geldversorgung zu ermöglichen. Das Finanzportal biallo.de hat die Gebühren aller knapp 400 Sparkassen Deutschlands genau unter die Lupe genommen. Das Portal stellte fest, dass immer mehr Sparkassen dazu übergehen, sich an ihren eigenen Schaltern und Automaten für das Geldabheben bezahlen zu lassen. Stefan Genth, Chef des Einzelhandelsverbands, sagte zu der neuen Praxis der Sparkassen: «Die Preispolitik der Banken lässt darauf schliessen, dass sie die Bargeldversorgung als Belastung sehen und sich davon langfristig verabschieden wollen.» Anscheinend soll das Bargeld so teuer gemacht werden, damit die bargeldlose Gesellschaft akzeptiert wird.

Quelle: Stimme und Gegenstimme 17/17

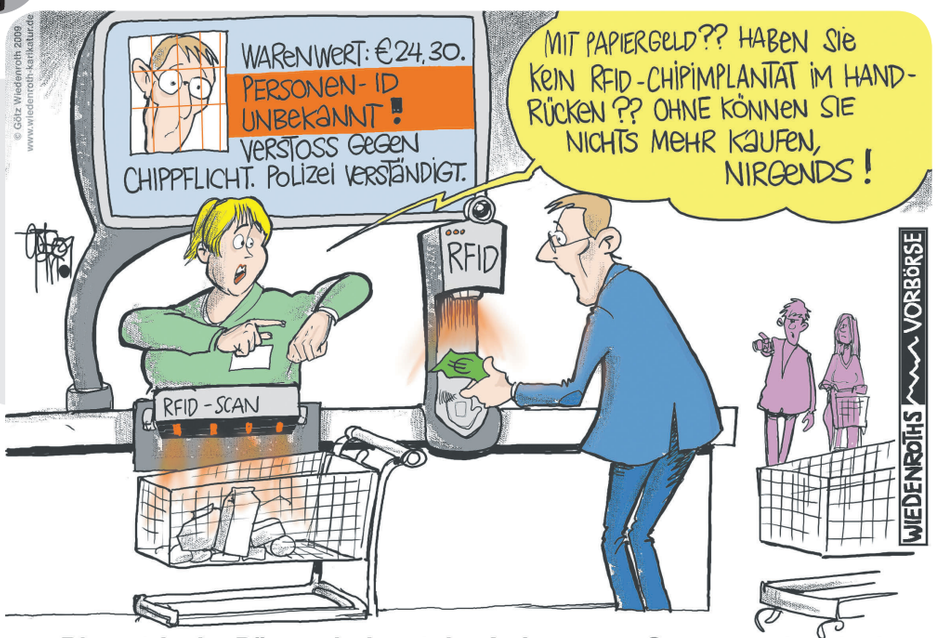
Modell Schweden?

Das Ganze ist beileibe keine innerschwedische Angelegenheit. Vielmehr erproben mehrere EU-Staaten die verschiedensten Bargeldverbote, darunter auch Staaten der Eurozone. Das Ticket in den totalen Überwachungsstaat ist die Finanzkrise. Um die Steuereinnahmen zu erhöhen und die staatliche Schuldenlast abzubauen, führte Griechenland ab 1. Januar 2011 eine weitgehend bargeldlose Gesellschaft ein. Nur noch Beträge bis 1500 Euro dürfen in bar bezahlt werden (bei geschäftlichen Transaktionen bis 3000 Euro). Zusätzlich werden umfangreiche Überwachungssysteme eingeführt, die den Bürger finanziell total durchleuchten sollen. «In Griechenland wird das Wirklichkeit, was viele Geldsystemkenner bereits als Gefahr prophezeit haben: Bankrotte Regierungen schaffen den totalen Überwachungsstaat, um Steuereinnahmen zu erhöhen», titelte die International Business Times am 16. Februar 2010. Griechenland handele nach der Devise: «Bargeld ist verdächtig.»

Dies dürfte das Ende der Demokratie in Europa einläuten. Denn die Massnahmen sind von oben abgesegnet. Vor ihrem Angriff auf das Bargeld fragten die Griechen extra die Europäische Zentralbank nach deren Meinung. Und die hatte – obwohl die Euro-Banknoten in den Euro-Staaten immerhin gesetzliches Zahlungsmittel sind – nichts dagegen. Der Trick: Das Ganze ist erlaubt, solange andere Zahlungswege offenstehen (Verordnung des Rates Nr. 974/98 vom 3. Mai 1998, Artikel 11). Schliesslich gebe es ja bereits Bargeldbeschränkungen, beispielsweise die, dass niemand gezwungen sei, mehr als 50 Münzen auf einmal zu akzeptieren. Der Weg in den bargeldlosen Überwachungsstaat ist also längst geebnet.

Quelle: Verheimlicht, Vertuscht, Vergessen 2011, Gerhard Wisnewki, Knaur

Ist es bald aus mit dem Bargeld?



Biometrische Pässe sind erst der Anfang vom Gouvernantenstaat

Wer am 31.03.2015 einen Blick auf die politische Analyse-Website konjunktion.info warf, könnte das glatt glauben: «Bargeldverbot: Das Fenster zum Widerstand schliesst sich», stand da zu lesen. Münzen und Scheine seien «ein im Sterben begriffenes Freiheitsgut, dem kontinuierlich die Lebensgrundlage entzogen» werde. Weltweit nähmen die «Restriktionen bezüglich des Bargeldeinsatzes zu», und «immer mehr Regierungen schieben ‚Sicherheitsbedenken' vor, um eine De-facto-Abschaffung des Bargelds zu erreichen. Terrorismus, Organisiertes Verbrechen, Steuerhinterzieher, Drogendealer oder Geldwäsche sind die beliebtesten Begründungsfloskeln zur Dämonisierung des Bargelds.» Die Abschaffung des Bargelds soll eine bessere Kontrolle von Zahlungsvorgängen ermöglichen: Denn Plastikkarten, PayPal und Banküberweisungen lassen sich staatlicherseits nun mal «leichter überwachen und sind dadurch natürlich die bevorzugten ‚Nachfolgeoptionen' auf dem Weg, Bargeld zu etwas ‚Verdächtigem zu machen'. Immer öfter wird man schräg angeschaut, wenn man grössere Summen bar bezahlen will und nicht sofort sklavisch irgendein Stück Plastik zückt. Was letztlich eine klassische Konditionierung darstellt und sich immer mehr ausbreitet.»

Der erste Schritt zu einem Bargeldverbot wurde schliesslich schon vor langer Zeit getan – mit der Einführung bargeldloser Zahlungssysteme. Diese Systeme könnten problemlos auch noch ein paar Millionen Zahlungsvorgänge mehr «verdauen», die zurzeit noch mit Bargeld abgewickelt werden. Die Schlinge zieht sich bedrohlich zu, und zwar nicht nur um den «Hals» unseres Bargeldes, sondern auch um unseren eigenen. Ohne Bargeld droht die totale Überwachung. Am 15. März 2013 zählte der Bundestagsabgeordnete Frank Schäffler auf:

- In Griechenland gilt seit Januar 2011 ein Verbot von Bargeldzahlungen über 1500 Euro für Privatpersonen und 3000 Euro für Geschäftsleute.
- Eine der ersten Amtshandlungen Mario Montis [Ministerpräsident] in Itali-

EU-Bevölkerung: Bargeldobergrenzen werden abgelehnt!

Im April 2017 startete die EU-Kommission eine öffentliche Umfrage zu Bargeldobergrenzen. Das Ergebnis dieser Umfrage hat es in sich: 95 % der Teilnehmer sprachen sich gegen Bargeldobergrenzen auf EU-Ebene aus. Für 87 % ist die Möglichkeit, anonym bezahlen zu können eine Grundfreiheit und drei Viertel sind der Meinung, dass Bargeldobergrenzen ineffektiv bei der Bekämpfung von Steuerhinterziehung, Terrorismus und Geldwäsche seien. Damit zeigt sich deutlich, wie klar die vorgebrachten Argumente für Bargeldobergrenzen von der Mehrheit durchschaut werden. Doch davon völlig unbeeindruckt werden Bargeldzahlungen in der EU weiter eingeschränkt. So wurde in Deutschland auf Vorgabe der EU am 26.6.2017 die Obergrenze für anonyme Bargeldzahlungen von 15.000 € auf 10.000 € gesenkt. Es stellt sich die Frage: Wozu wird die Bevölkerung überhaupt noch nach ihrem Willen gefragt?

Quelle: Stimme und Gegenstimme 01/2018
derstandard.at, EU-Bargeldobergrenze wird massiv abgelehnt, 13.06.17

Ohne Smartphone zahlungsunfähig

Foto: HLundgaard https://commons.wikimedia.org/wiki/File:Mobile_Payment.jpg (https://creativecommons.org/licenses/by-sa/3.0/deed.en)

Wohin bargeldloses Zahlen führen kann, zeigt sich in China schon sehr deutlich. Dort besitzen viele Bürger kein Bargeld mehr. Stattdessen werden von Jung und Alt alle Zahlungen per Smartphone erledigt. Über eine App kann man selbst an kleinsten Essensständen schnell und bequem die Rechnung begleichen. Teilweise geht es jedoch schon so weit, dass man nur noch auf diesem Weg bezahlen kann. Möchte man z.B. eines der Fahrräder ausleihen, die an allen Ecken angeboten werden, ist das nur auf dem eben beschriebenen Wege möglich. Wer über diese App nicht verfügt, hat Pech gehabt und muss auf den Fahrradverleih verzichten. Was heute «nur» das Fahrrad betrifft, können morgen vielleicht schon lebenswichtige Dinge sein.

Quelle: Stimme und Gegenstimme 41/17

Die Bargeldabschaffung wird von der Finanzelite massiv vorangetrieben

Foto: World Economic Forum (https://commons.wikimedia.org/wiki/File:BillGates2012.jpg) https://creativecommons.org/licenses/by/2.0/deed.en

Ende 2015 verkündete Bill Gates auf einer Tagung des US-Finanzministeriums, dass seine Stiftung bis Ende 2018 den Zahlungsverkehr in Indien, Pakistan und Nigeria komplett auf bargeldlos umgestellt haben will. Bereits seit 2012 arbeite er gemeinsam mit der indischen Zentralbank an diesem Ziel. Zu diesem Zweck gründete die Gates Stiftung, zusammen mit der US-Behörde für Entwicklungshilfe, die «Better Than Cash Alliance», eine Allianz zur Bargeldabschaffung. Mitglieder dieser Allianz sind 50 Firmen und Organisationen vor allem aus dem Finanzdienstleistungssektor. Der Leiter dieser US-Entwicklungshilfebehörde, Rajiv Shah, wurde nach der erfolgreichen indischen Bargeldreform im Jahr 2016 zum Präsidenten der Rockefeller Stiftung ernannt. Offensichtlich hatte er seinen Job gut gemacht. Das Beispiel Indiens zeigt, wie hinter den Kulissen die weltweite Abschaffung des Bargelds massiv vorangetrieben wird. Es zeigt aber auch, wie hoch der Einfluss der Superreichen auf Regierungen und oberste Entscheidungsträger sein muss, dass z.B. Bill Gates die Politik von Ländern wie Indien nach seinen Wünschen beeinflussen kann.

Quelle: Stimme und Gegenstimme 01/2018

Totale Kontrolle durch Bargeldabschaffung

Auf dem Weltwirtschaftsforum Anfang 2017 in Davos verkündete Amitabh Kant, Chef von Indiens führender Wirtschaftsförderungsbehörde, die Einführung biometrischer Zahlungen in Indien innerhalb von drei Jahren. Hierzu startete Indien bereits 2010 ein Programm mit dem Ziel, die biometrischen Daten aller 1,2 Milliarden Inder zu erfassen. Dies umfasst die Registrierung aller zehn Fingerabdrücke, die Aufnahme der Netzhaut beider Augen und ein frontales Gesichtsbild. Durch die radikale Bargeldreform, die Indiens Regierung schon im November 2016 durchführte, wurde die gesamte Bevölkerung dazu gezwungen, ihre biometrischen Daten erfassen zu lassen. Ungültig gewordene Banknoten konnten nur noch über ein eigenes Bankkonto umgetauscht, und dieses wiederum nur bei gleichzeitiger Erfassung aller biometrischen Daten eingerichtet werden. Durch die Bargeldabschaffung wird die Bevölkerung nicht nur ihres Bargeldes beraubt, sondern sie wird vollkommen kontrollier- und beherrschbar. Wird diese Art der Zahlung in Indien etwa getestet, um sie bald weltweit einzuführen?

Quelle: Stimme und Gegenstimme

en war im Dezember 2011 die Einführung einer Obergrenze für Bargeldtransaktionen von 1000 Euro.

- In Spanien sind seit November 2012 Bargeldgeschäfte über 2500 Euro verboten.
- Auch Frankreich plant ein Verbot von Barzahlungen über 1000 Euro ab 2014. Schon heute gilt dort im Regelfall ein Maximum von 3000 Euro.
- In Schweden fordern Gewerkschaften, Unternehmen und Behörden ein komplettes Bargeldverbot. [1].

Sollte das Bargeld tatsächlich verschwinden, würde jeder einzelne Zahlungsvorgang überwachbar. Und da fast alles im Leben Geld kostet, wäre unser Leben ohne Bargeld künftig wie ein offenes Buch.

Abstumpfung statt Aufklärung

Das Problem ist, dass man mit dem Thema Überwachung im Zeitalter von Facebook und Smartphone nur schwer jemanden hinter dem Ofen hervorlocken kann. Selbst ein Edward Snowden sorgte schliesslich nicht in erster Linie für Aufklärung, sondern für Abstumpfung. Wer macht sich im Zeitalter der totalen digitalen Durchleuchtung und des totalen Exhibitionismus noch Gedanken über Überwachung? Die Geheimdienste wissen inzwischen mehr über uns als wir selbst. Metaanalysen der von uns verbreiteten Daten erlauben tiefere Einblicke in unsere Seele, als wir glauben. Schon die blossen Begriffe, die wir in unseren Postings und Internet-Beiträgen benutzen, lassen tief blicken. Unsere Vorlieben und Abneigungen sind im Netz für alle transparent. Und auf Zahlungsvorgänge trifft diese Transparenz natürlich genauso zu. Allein anhand unserer Online-Einkäufe lässt sich ein umfassendes Lebens- und Persönlichkeitsbild von uns zeichnen. Aber um die Wahrheit zu sagen: Die Überwachung ist beim Gegenstand Bargeldverbot noch nicht einmal das eigentliche Thema. Über die wirklichen Konsequenzen berichtet nämlich schon gar niemand: Das ausschliesslich elektronische Zahlungssystem wäre der Einstieg in die totale Sklaverei. Jedermann würde sofort auf den Knien herumrutschen, nur um wieder zahlen zu können.

Quellen: 1. frankschaeffler. de, 15.3.2013
Verheimlicht, Vertuscht, Vergessen 2016, Gerhard Wisnewki, Knaur

Folgen der Bargeldabschaffung

In einer digitalen Welt ohne Bargeld würden Alkoholkonsum, Rauchgewohnheiten, Medikamentenkonsum, Kondom- und Hygieneartikelverbrauch, Finanzverhalten, Essgewohnheiten, Freizeitverhalten, Benutzung öffentlicher Toiletten und anderer kostenpflichtiger Einrichtungen minutiös und lückenlos bis in die intimsten Bereiche erfasst. Also vorbei mit Privatsphäre! Jeder Mensch würde angreif- und manipulierbar! Dem politischen System missliebige Menschen können kurzerhand durch Kontosperrung per Knopfdruck vom gesellschaftlichen Leben abgekapselt werden. Ohne Zahlungsfähigkeit wäre man nicht mehr existenzfähig; der Mensch wäre ein regelrechter Sklave der Banken und des gesamten, von der Finanzoligarchie vorangetriebenen, Systems. Bei stets möglichen Bankenpleiten ist die Vernichtung jeglichen Sparvermögens unumgänglich, da die Einlagensicherung der Banken niemals ausreichen würde, den entstandenen Verlust auszugleichen. Noch Fragen?

Quelle: Stimme und Gegenstimme 04/2018

Verkehr

Überwachung

- Nach den Wünschen von Politik und Grosskonzernen soll das Auto der Zukunft dem Fahrer jegliche Eigenverantwortung nehmen und automatisch von einem Bordcomputer gesteuert werden. Das Aufgeben der Verantwortung birgt jedoch grosse Risiken: Wer nicht selbst steuert, unterwirft sich sowohl der Überwachung als auch der Kontrolle anderer.
- Der ADAC fand heraus, dass moderne Autos ihren Herstellern via Sim-Karte massenweise Daten senden. Die Untersuchung zeigte u.a., dass neben der Position des Fahrzeugs oder Zielen im Navigationssystem sogar Kontaktdaten der Handys von Insassen auf den Servern der Autohersteller landen.
- Autohersteller können heute schon auf das einzelne Auto aus der Ferne zugreifen. Renault kann beispielsweise beim Elektroauto Zoé das Aufladen der Antriebsbatterie verhindern. Das zeigt, wie leicht den Fahrern schon jetzt die Souveränität über ihr Fahrzeug entzogen werden könnte.
- Wie es scheint, werden in Zukunft Hersteller, Versicherer und höchstwahrscheinlich auch der Staat auf die eigentlich privaten Daten über die Position und das Verhalten des Fahrers zugreifen können. Garantieleistungen könnten verwehrt bzw. Versicherungsprämien erhöht werden, weil die Hersteller bzw. Versicherer Informationen über das risikoreiche Fahrverhalten des Automobilbesitzers erhalten. Sobald der Staat Zugriff auf diese Daten bekäme, bräuchte es keine Blitzer und Verkehrspolizisten mehr, denn jede Geschwindigkeitsüberschreitung könnte dann einfach digital bestraft werden, wie Justizminister Heiko Maas es sogar schon angedeutet hat.
- Der nächste Schritt wäre dann das selbstfahrende Auto. Eine technische Utopie, mit der es anscheinend gar nicht schnell genug gehen kann. Die vorhandene Technologie, die eigentlich noch jahrzehntelange Forschungsarbeit bräuchte, um auszureifen, wird der Öffentlichkeit momentan im Eiltempo aufgedrückt, ohne dass man die Autofahrer je nach ihrer Meinung gefragt hätte.
- Warum die Politik das selbstfahrende Auto kaum noch erwarten kann, lässt sich erahnen: Da die Freiheiten, die ein normales Auto bietet, den Regierenden ein Dorn im Auge sein könnten, könnte es jetzt schnellstmöglich darum gehen, eine Technologie zu entwickeln und unters Volk zu bringen, bei der letztlich der Staat am Steuer sitzt. Der Staat würde einfach einen Code benutzen, um sich in den Bordcomputer einzuklinken und könnte somit jederzeit die Kontrolle des Fahrzeugs übernehmen.

Foto: Shutterstock/chombosan

Wie Autohersteller unsere Daten sammeln

Laut einem Bericht des SRF hat der deutsche ADAC in einer aufwendigen Analyse vier Fahrzeug-Modelle von drei Automarken genauer untersucht: Einen Mercedes der B-Klasse, einen Renault Zoé sowie zwei Modelle von BMW, das Elektromobil i3 und den 320.

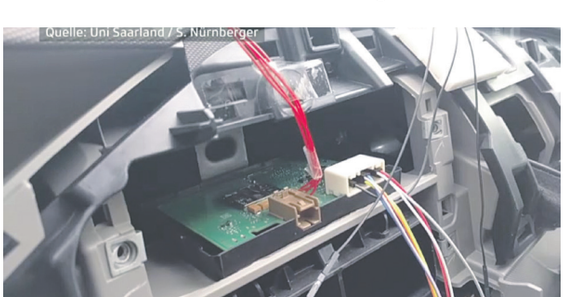
«Bei den vier Fahrzeugen, die wir untersucht haben, waren wir überrascht, welche Mengen an Daten erzeugt und übertragen werden und dass gegenüber dem Konsumenten keinerlei Details vermittelt werden», fasst Arnulf Thiemel gegenüber dem SRF die insgesamt zweijährige Untersuchung zusammen.

«Da werden regelmässig ganze Datenpakete an den Hersteller geschickt, bei denen wir uns weder mit böswilligster noch mit gutwilligster Betrachtungsweise vorstellen können, was die Hersteller damit anfangen wollen», erklärt Thiemel.

Die Recherche des ADAC zeigt auch, dass sogar Kontaktdaten des Handys auf den Server des Autoherstellers geschickt werden.

In modernen Autos stecken bis zu 200 Sensoren. Diese erheben bei jedem Fahrkilometer unzählige Daten.

Foto: S 400 HYBRID (https://commons.wikimedia.org/wiki/File:Mercedes_C_200_Kompressor_Elegance_(W204)_front_20100603.jpg)



Via eingebauter Sim-Karte sendet das Auto über Mobilfunk automatisch ganze Datenpakete zum Hersteller. Dieser erfährt so vieles über Fahrzeug und Halter. Foto: SRF

und Entmündigung durch moderne Autos

Oder welche Musik der Autofahrer abgespielt hat. Diese Daten seien besonders problematisch, weil sie Aufschluss über den Nutzer des Autos geben würden, so Thiemel.

Hersteller-Zugriff aus der Distanz

Äusserst brisant: Autohersteller können auch auf das individuelle Auto aus der Ferne zugreifen. Renault kann beispielsweise beim Elektroauto Zoé das Aufladen der Antriebsbatterie verhindern. «Der Fahrzeughersteller kann sogar den Antriebs-Akku abschalten. Und zwar dann, wenn Sie beispielsweise Ihre Leasinggebühr für den Akku nicht bezahlt haben», unterstreicht Arnulf Thiemel vom ADAC. So könnte Renault verhindern, dass das Auto wieder aufgeladen werden kann.

Renault schreibt hierzu an den SRF: «Die Unterbindung des Ladevorgangs eines Renault Zoé per Mobilfunkverbindung ist bei Schweizer Renault Privatkunden noch nie eingesetzt worden.» Im extremen und unwahrscheinlichen Fall sowie nach mehrmaliger Kontaktaufnahme mit dem Fahrer könne Renault den Ladevorgang unterbinden. Das ändert jedoch nichts daran, dass die Technik zur Deaktivierung aus der Ferne bereits voll funktionsfähig ist.

Intransparente Autofirmen

Die vom ADAC untersuchten Automarken Renault, Mercedes und BMW behaupten alle, sie hielten sich an die Datenschutzbestimmungen. Der Käufer stimme dem Daten-Austausch beim Kauf zu und er würde an mehreren Orten transparent darüber informiert. Eine Auflistung aller erhobenen Daten liefern die Hersteller nicht.

Eine Umfrage des SRF bei den zwölf Automarken, die in der Schweiz am häufigsten verkauft werden, verlief sehr ernüchternd. Auch nach mehrmaligem Nachfragen schafften es drei Anbieter nicht, klare Antworten zu liefern. Die simple Frage lautete: Welche Daten werden bei Ihrem meistverkauften Modell sowie bei Ihrem neusten Modell erhoben, verarbeitet, gespeichert und extern übermittelt?

Klar äussert sich Toyota: Man verbaue keine SIM-Karten in den Autos. Eine Datenübermittlung sei somit ausgeschlossen. Und Opel liefert als einzige Marke eine nahezu vollständige Übersicht der gesammelten und gesendeten Daten inklusive Verwendungszweck.

Alle anderen Autobauer schreiben sinngemäss, dass ihnen Transparenz wichtig sei und sie nach geltenden Datenschutzrichtlinien handeln würden. Ausserdem würde die Käuferschaft dem Datenaustausch ausdrücklich zustimmen.

Das und vieles mehr erfahren die Hersteller über das Verhalten der Fahrzeuginsassen:

Die GPS-Daten des Navigationsgerätes verraten dem Hersteller, wo der Fahrer unterwegs ist.

Auch über Kilometerstand, Verbrauch und Tankinhalt weiss der Hersteller bescheid.

Wie oft wird der Gurtstraffer aktiviert, weil der Fahrer zu heftig bremst?

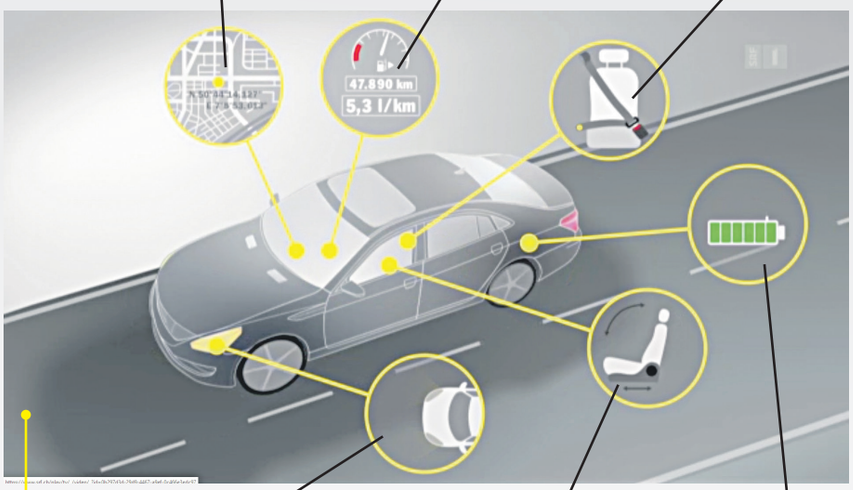


Foto: SRF

Daten über das Licht sagen, zu welcher Tageszeit das Auto unterwegs ist.

Wird der Fahrersitz oft verstellt, weiss der Hersteller, dass mehrere Lenker das Auto benutzen.

Das Auto sendet auch Angaben zur Batterie. Diese verraten, wie oft und wie lange gefahren wird.

All diese Daten können auf den Servern der Fahrzeughersteller landen...

...und ein detailliertes Nutzungsprofil ergeben.

BMW 320d

Foto: M 93 (https://commons.wikimedia.org/wiki/File:BMW_320d_Touring_(F31)_%E2%80%93_Frontansicht,_11._Februar_2013,_D%C3%BCsseldorf.jpg) https://creativecommons.org/licenses/by-sa/3.0/de/deed.en

- Maximaldrehzahl des Motors mit jeweiligem Kilometerstand (erlaubt Rückschlüsse auf den Fahrstil)
- **Fahrstrecken**
- Dauer der Fahrt in den jeweiligen Modi des Automatikgetriebes (Rückschlüsse auf Fahrstil)
- Betriebsstunden der Fahrzeugbeleuchtung, getrennt nach Lichtquellen
- Zahl der Fahrersitz-Justierungen (erlaubt Rückschlüsse auf Anzahl Fahrer)
- Anzahl der eingelegten Medien ins CD-/DVD-Laufwerk
- Zahl der elektromotorischen Gurtstraffungen z.B. aufgrund starker Bremsmanöver (Erlaubt Rückschlüsse auf den Fahrstil)
- **Bei Anbindungen des Handys via Bluetooth Kontaktdaten (je nach Telefonmodell)**
- **Ins Navigations-System eingegebene Ziele**

BMW i3 (Elektroauto)

Foto: TTTNIS (https://commons.wikimedia.org/wiki/File:BMW_i3_01.jpg) https://creativecommons.org/publicdomain/zero/1.0/deed.en

- Detaillierte Daten der Antriebsbatterie (wie Ladezustand, Zelltemperatur usw.)
- Gewählter Fahrmodus (eco, eco plus, sport)
- Wie oft wurde der Ladestecker eingesteckt?
- Wie und wo wurde geladen, wie stark war die Antriebsbatterie entladen
- Kilometerstand bei Bedienvorgängen wie z.B. Laden
- Position der 16 zuvor benutzten Ladestationen
- **Rund 100 letzte Abstellpositionen des Fahrzeugs**
- **Telefonkontakte des Handys des Fahrers**
- **Abgespielte Musiktitel**

Mercedes-Benz B-Klasse

Foto: Matthias93 (https://commons.wikimedia.org/wiki/File:Mercedes_B-Klasse_Sportpaket_front.jpg) https://creativecommons.org/licenses/by-sa/3.0/deed.en

- **Etwa alle zwei Minuten werden die GPS-Position des Autos sowie Statusdaten an den Hersteller übertragen (unter anderem Kilometerstand, Verbrauch, Tankfüllung, Reifendruck sowie Füllstände von Kühlmittel, Wischwasser oder Bremsflüssigkeit)**
- Gespeichert wird die Anzahl der Gurtstraffungen (erlaubt Rückschlüsse auf den Fahrstil)
- Fehlerspeichereinträge werden teilweise mit Informationen über zu hohe Motordrehzahl oder -Temperatur abgelegt (erlaubt Rückschlüsse auf den Fahrstil)
- Fahrkilometer auf der Autobahn, ausserorts und in der Stadt werden getrennt gespeichert (erlaubt Rückschlüsse auf das Nutzungsprofil)
- Betriebsstunden der Fahrzeugbeleuchtung werden gespeichert
- Die letzten 100 Lade- und Entladezyklen der Starterbatterie werden mit Uhrzeit, Datum und Kilometerstand gespeichert. Daraus ergeben sich Fahr- und Standzeiten.

Renault Zoe (Elektroauto)

- **Aufladen der Antriebsbatterie kann von Renault via Mobilfunkverbindung jederzeit unterbunden werden. Der Autobauer kann also aus der Ferne auf das Auto zugreifen. Was wäre, wenn sich der Hersteller in der Zukunft das Recht herausnehmen würde, den Antriebsakku abzuschalten, z.B. bei nicht gezahlten Leasing-Gebühren?**
- Bei jeder Fahrt, spätestens nach jeweils 30 Minuten, wird ein Datenpaket (u.a. Fahrgestellnummer, div. Seriennummern, Datum, Uhrzeit, GPS-Position, Temperatur, Ladung und Zellspannung der Hochvolt-Antriebsbatterie) an Renault gesendet. Der Hersteller kann die Informationen jederzeit anfordern.

Foto: Clément Bucco-Lechat (https://commons.wikimedia.org/wiki/File:Geneva_MotorShow_2013_-_Renault_Zoe_charging.jpg) https://commons.wikimedia.org/wiki/User:Pleclown

srf.ch, Datenkrake Auto – Wie uns Autobauer ausspähen, 21.02.2017

Zwangseinführung des eCall-Notrufsystems: Lückenlose Überwachung des Autos ab 2018

Ab 2018 wird das automatische Notrufsystem eCall in allen neuen Pkw-Modellen in der EU zur Pflicht. Das EU-Parlament stimmte am 28.04.2015 abschliessend für das neue System, mit dem nach Schätzungen der EU-Kommission die Zahl der Unfalltoten um zehn Prozent verringert werden könnte.

Bei einem Unfall soll eCall automatisch den einheitlichen europäischen 112-Notruf auslösen. So sollen Helfer schneller zum Unfallort geführt werden – auch wenn der Fahrer bewusstlos ist. Die elementaren Bestandteile dieser ab 2018 für jeden Neuwagen verordneten Technologie sind ein GPS- und ein GSM-Modul zur Positionsbestimmung und für den Aufbau einer Daten- und Telefonverbindung.

Die eCall-Kritikerin Nadja Hirsch aus dem EU-Parlament erläuterte dem ARD-Magazin «Fakt» 2014, dass eCalls Überwachungsmöglichkeiten jedoch über Notrufe hinausgehen: «Die Kommission hat jetzt schon ganz klar gesagt, dass dieser Mechanismus auch genutzt werden kann, um gestohlene Autos zu finden. Das macht klar, dass die Sim-Karte jederzeit von aussen aktiviert werden kann, und das heisst natürlich: Wenn eben irgendjemand anderes – egal ob es ein Geheimdienst ist, eine Polizei, ein Steuerfahnder, dergleichen – dich finden will, wird er diesen Mechanismus dann aktivieren.»

Die Mehrheit des EU-Parlaments stimmte gegen die Option, dass das System vom Fahrer deaktiviert werden könnte. «Der Verbraucher hat gar keine Wahl mehr. Er hat nicht die Wahl, ob es eingebaut wird oder nicht, und er hat auch nicht mehr die Wahl, ob dieses System, wenn es denn eingebaut ist, an – oder ausgeschaltet werden kann», kritisiert Hirsch.

Diese Verordnung ist symptomatisch für die Geisteshaltung der EU-Eliten und «Digitalisierer». Dem Verbraucher wird versprochen, es ginge um seine Sicherheit und deshalb müsste man ihn zu seinem Glück zwingen. Über die eigentlichen Wünsche des Verbrauchers wird achselzuckend hinweggesehen. Er hat nicht die Wahl zwischen mehr Freiheit oder mehr Sicherheit, seine Sicherheit wird ihm von oben aufgezwungen und perfide als «Modernisierung» verkauft.

Doch nach der antidemokratischen und destruktiven Politik (Grenzöffnung, Euro-Krise usw.) der letzten Jahre will man der EU nicht mehr so recht glauben, ihr läge die Sicherheit ihrer Bürger am Herzen. So schlussfolgert sogar die ARD: «Ebenso ging es mit der Abschaffung des Bankgeheimnisses. Zunächst sollten dadurch Terroristen gejagt werden, was erfolglos blieb. Drei Jahre später konnten die Finanzämter und Sozialbehörden auf die Kontodaten schauen, wovon massenweise Gebrauch gemacht wird. Sicherheit dient regelmässig als Türöffner.»

Die Abgeordnete Hirsch bemerkt abschliessend: «Wir merken sehr stark, dass […] immer der Sicherheitsaspekt nach vorne geschoben wird, um die Freiheit der Menschen und auch die freie Entscheidung des Verbrauchers immer stärker einzuengen. Wir werden niemals hundertprozentige Sicherheit haben, aber was man hundertprozentig sagen kann, ist, dass die Freiheit immer stärker eingeschränkt wird.»

Quellen: epochtimes.de, eCall im Auto: Back to the future – die totale Überwachung, 29.04.2015
Youtube.com, E-Call wie die EU Autofahrer ausspionieren will, 08.04.2014

Heiko Maas warnt vor Daten-Sammelwut bei intelligenten Autos

Foto: Sandro Halank, Wikimedia Commons, CC-BY-SA 3.0

Ausgerechnet er? Bundesjustizminister Heiko Maas (SPD) mahnte 2015, dass bei der zunehmenden Digitalisierung des Autofahrens der Mensch die Hoheit über seine Daten behalten müsse. «Smart Cars bieten faszinierende Möglichkeiten», schrieb der SPD-Politiker in einem Gastbeitrag für das «Handelsblatt». Immer mehr Kfz-Versicherer böten Tarife an, bei denen jene einen Rabatt bekommen, die in die digitale Überwachung des eigenen Fahrverhaltens einwilligen. «Wenn solche Tarife zum Regelfall werden, wird die Freiheit des unkontrollierten Fahrens ein kostspieliger Luxus oder ganz unmöglich», so Maas.

Noch gehe es nur darum, Schadensfälle zu vermeiden, aber vorhandene Daten weckten stets Begehrlichkeiten. «Bewegungs- und Verhaltensprofile könnten erstellt werden, über die jeder Strafverfolger frohlocken würde», schreibt Maas und fügt hinzu: **«Mit der Datenübertragung in Echtzeit könnte der Fahrer vielleicht auch digital zur Einhaltung der Verkehrsregeln angehalten werden».** An die Industrie richtete Maas deshalb Forderungen zum Auto der Zukunft: Schon bei der Entwicklung müsse der Datenschutz berücksichtigt werden, Datenvermeidung und Datensparsamkeit müssten leitende Grundsätze sein. Ferner solle der Fahrer der Datensammlung ausdrücklich zustimmen. Auch müsse es einen «Aus-Knopf» geben: Dem Fahrer müsse es möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und zu stoppen. Fünftens solle jeder frei wählen können, welches Unternehmen Zugriff auf die Daten bekommt. Zudem solle Missbrauch und Manipulation verhindert werden. Schliesslich müssten jene Systeme, die für den Fahrer das «Denken» übernehmen, sicher sein.

Aus Maas' Mund, der nicht umsonst in Deutschland den Spitznamen «Überwachungsminister» weg hat, klingen diese eigentlich vernünftigen Aussagen wenig glaubwürdig. Handelt es sich dabei etwa um skrupellose Lügen, um dem Wahlvolk die Digitalisierung schmackhaft zu machen? Vor allem Maas' Szenario der digitalen Verkehrskontrolle bestätigt die Vorbehalte der Datenschützer gegen die Digitalisierung des Verkehrs.

Quelle: epochtimes.de, Maas warnt vor Daten-Sammelwut bei intelligenten Autos, 13.06.2015

Totalüberwachung beim Autofahren – Versicherer berechnen Tarif nach Fahrstil

Mehrere Versicherer testen die Einführung sogenannter Telematik-Tarife. Das heisst, das Auto kommuniziert ohne das Wissen des Fahrers mit der Versicherung und speichert u.a. das Fahrverhalten. Dabei wird der Fahrstil, also beispielsweise das Beschleunigungs- und Bremsverhalten, eines Versicherten aufgezeichnet, übermittelt und ausgewertet. Die Idee dahinter: Wer vernünftiger fährt, soll weniger bezahlen.

Aus den Daten lassen sich exakte Verhaltens- und Bewegungsprofile des Fahrers erstellen. Viele Firmen haben daran grosses Interesse: der eigene Arbeitgeber, das Finanzamt, Versicherungen, Autowerkstätten, Fahrzeughersteller, Gesundheitsdienstleister. Vielleicht auch die Maut-Behörde und Geheimdienste.

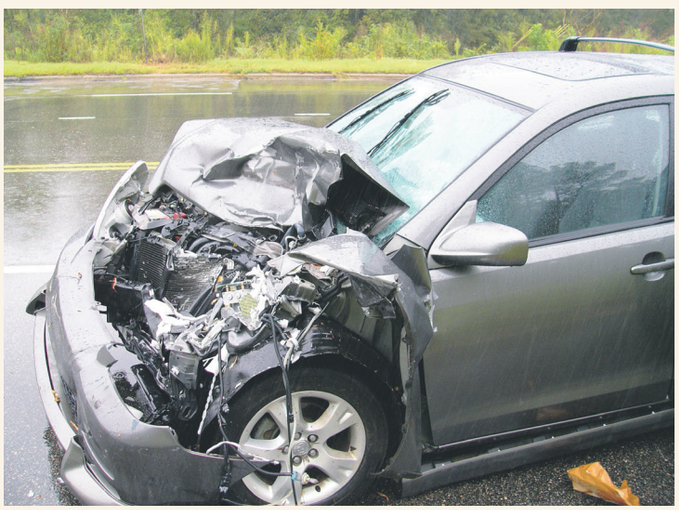


Foto: W. Robert Howell from Charlotte, NC, United States (https://commons.wikimedia.org/wiki/File:Car_Accident.jpg)

Konkret ist das von folgenden Versicherungen bekannt:

- Die HUK-Coburg bestätigt, dass sie entsprechende Aufzeichnungsgeräte testet.
- Die Allianz arbeitet in Italien schon seit Jahren mit Telematik-Tarifen und beobachtet die Entwicklung in Deutschland. «Wir sind der Meinung, dass die deutschen Autofahrer einen Telematik-Tarif annehmen werden, sofern er die Datensicherheit der Kunden sicherstellt und deutliche Vorteile für die Zielgruppe bringt», sagte Allianz-Vorstand Alexander Vollert.
- S-Direkt, die Sparkassen Direktversicherung (in Zusammenarbeit mit O2) lässt die Daten einer Auto-«Blackbox» von einem externen Dienstleister in einen Punktwert umrechnen, und sinkt dieser, bezahlt der Autofahrer weniger.
- Die Webseite Versicherungsbote.de nennt noch die VHV, Itzehoer sowie Axa, die im Herbst 2015 damit begonnen haben.

Quelle: epochtimes.de, Totalüberwachung beim Autofahren – Versicherer berechnen Tarif nach Fahrstil, 15.07.2015

Zusammenfassend lässt sich feststellen: Viele moderne Autos verfügen schon über die Technik zur totalen Überwachung der Insassen. Wie es scheint, werden in Zukunft Hersteller, Versicherer und höchstwahrscheinlich auch der Staat auf die eigentlich privaten Daten über die Position und das Verhalten des Fahrers zugreifen können. Garantieleistungen könnten verwehrt bzw. Versicherungsprämien erhöht werden, weil die Hersteller bzw. Versicherer Informationen über das risikoreiche Fahrverhalten des Automobilbesitzers besitzen. Dass die Autohersteller für die vom SRF aufgedeckte Verletzung der Privatsphäre ihrer Kunden nicht bestraft werden, lässt vermuten, dass die Dauerüberwachung politisch erwünscht ist. Die Regeln des Strassenverkehrs ohne negative Konsequenzen zu brechen, könnte mit diesen technischen Möglichkeiten bald nicht mehr möglich sein. Sobald der Staat Zugriff auf diese Daten bekäme, bräuchte es keine Blitzer und Verkehrspolizisten mehr, denn jede Geschwindigkeitsüberschreitung könnte dann einfach digital bestraft werden, wie Heiko Maas es sogar schon angedeutet hat. **Man muss kein Gegner von (Verkehrs-)Regeln sein, um zu erkennen, dass diese Art der Dauerüberwachung und des ständigen Zwangs zu fehlerlosem Verhalten charakteristisch für totalitäre Systeme ist, deren Bürger sich mehrheitlich zu politisch angepassten Drohnen entwickeln, die brav alle Befehle der Regierung befolgen (siehe China).**

von Gerhard Wisnewski

Auto der Zukunft: Selbst fahren verboten!

Haha, das ist doch unmöglich, werden Sie sagen: ein Auto ohne Lenkrad und Pedale! Wo gibt's denn so etwas! Na – bei uns! Das selbstfahrende Auto sei jetzt «in aller Munde», stellte das Industriemagazin am 9. Januar 2017 fest. «Audi und Nvidia entwickeln gemeinsam selbstfahrendes Auto», hiess es am 5. Januar 2017 auch auf der Website Automobil Produktion. «Im Falle, dass keinerlei manuelles Steuern seitens des Fahrers nötig ist, wird auch der Begriff Roboterauto verwendet. Dann kann der Fahrersitz leer bleiben; eventuell sind Lenkrad, Brems- und Gaspedal nicht vorhanden», heisst es bei der Autoseite automat.ch (03.10.2016). Besonders «Google baute Prototypen ohne Lenkrad, Bremse und Gaspedal» [1].

Plötzlich kann es mit dieser technischen Utopie gar nicht mehr schnell genug gehen. «In fünf Jahren werden Sie in Roboterautos fahren», verkündete Google-Mitgründer Sergey Brin schon 2012 [2]. Tesla- Chef Elon Musk gab 2016 «zu Protokoll, dass er ein serienreifes, voll autonomes Fahrzeug bereits Ende 2017 sehe» [3]. Im selben Jahr 2016 kündigten auch BMW und Ford für 2021 autonome Fahrzeuge an [3]. Eifrig erwecken manche Medien sogar den Eindruck, das selbstfahrende Auto gebe es schon: «Fiat, Chrysler und Alphabet bringen Android Nougat ins selbstfahrende Auto», schrieb die Nachrichtenseite horizont.net (03.01.2017). «Volkswagen stellt erstes selbstfahrendes Auto vor», meldeten auch die Deutschen Mittelstands Nachrichten (online, 07.03.2017).

Schöne, neue Autowelt

Angeblich winkt uns damit die schöne, neue Autowelt. «Selbstfahrende Autos schaffen laut dem US-Forschungsinstitut Rand einen Mehrwert für die Gesellschaft», hiess es auf der Website pressetext.com (08.01.2014). «Laut dem Forschungsinstitut übertreffen die Vorzüge, die autonom betriebene Fahrzeuge mit sich bringen, die möglichen Nachteile bei Weitem.» «Der Nutzen für alle wäre gross», jubelte die Frankfurter Allgemeine Zeitung, «der Strassenverkehr würde sicherer, sind doch weit mehr als 90 Prozent aller Unfälle auf menschliches Versagen zurückzuführen» (online, 02.06.2015). «Wenn Autos mit Sensoren ausgestattet werden, die die Umgebung scannen und so schneller reagieren, rechnen Experten damit, dass sich die Zahl der Unfälle dramatisch reduziert», so Die ZEIT am 8. März 2014 (online): «Wenn es die Technologie schon gäbe, gäbe es keine Verkehrsunfälle und keine Staus mehr», zitiert das Blatt einen Experten des Wirtschaftsprüfungsnetzwerks Ernst & Young. «Ich kann dadurch die Zahl der Verkehrstoten auf null senken.» Hosianna! Schon tanzen wir um das selbstfahrende Auto wie weiland die Israeliten um das Goldene Kalb. Ist das eine gute Nachricht, die man uns hier vorzugaukeln versucht? Denn «selbstfahrend» heisst ja nun mal, dass nicht mehr wir fahren, sondern jemand anders das tut. Aber wer? Ganz einfach:

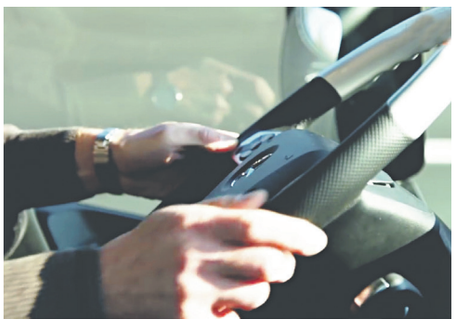
1. ein Computer,
2. Big Brother,
3. beide.

Foto: Shutterstock/LifetimeStock

«Wollen Sie diesen Unfall auch an Microsoft melden?»

Das kann uns nicht gefallen, denn was sind selbstfahrende Autos anderes als Hard- und Software? Man stelle sich vor, man würde sein Leben zum Beispiel einem Windows-Computer anvertrauen! Wir freuen uns schon auf blöde Fragen wie: «Wollen Sie diesen Unfall auch an Microsoft melden?» «Fehlerberichte» und «Problemlösungen» gibt es schliesslich nur, weil es Fehler und Probleme gibt. **Fehlerfreie Software zu produzieren ist prinzipiell nämlich unmöglich – ausser vielleicht in einem Taschenrechner. Und ein Auto, das von einem Computer gesteuert wird, kann nun mal «abstürzen» wie jeder andere Computer auch.** Dem menschlichen Dilemma entkommt man damit nicht, denn schliesslich sind ja auch Computer menschliche Produkte. Also können und werden sie auch versagen. Was zumindest jahrzehntelange Forschungsarbeit bräuchte, um auszureifen, soll nun plötzlich hopplahopp geschehen.

Und vor lauter Eile macht man den zweiten Schritt vor dem ersten, wie einige spektakuläre Unfälle mit vermeintlich selbstfahrenden Autos beweisen. Am 07.05.2016 zum Beispiel raste ein automatisch gesteuerter Tesla unter einen abbiegenden Sattelschlepper. Der Fahrer war sofort tot. Der Autopilot hatte von dem Lkw nur die grosse weisse Seite des Aufliegers wahrgenommen und sie für ein hoch hängendes Werbeplakat gehalten. Kurz: Ein solches Fahrzeug kann Sie auch umbringen.



Ob ein Computer jemals Erkenntnis und Urteilsvermögen eines menschlichen Fahrers ersetzen kann?

Seite 37

Selbststeuerung in Wahrheit ein Fahrassistenzsystem

«Ich bin der stolze Besitzer eines 2015er-Tesla SP90D, den ich mit allen verfügbaren Optionen gekauft habe», schrieb ein YouTube-Nutzer am 15. Oktober 2015 unter sein Video. «Es ist das beste Auto, das ich je besessen habe, und ich liebe es sehr. Ich besitze auch eine Menge Tesla-Aktien. Heute erhielt mein Auto das erwartete Software-Update der Version 7, und ich war bestrebt, den Autopiloten in der Nähe meines Hauses auszuprobieren. Nach einigen Sekunden freihändiger Fahrt brach die Hölle los. [...] Kurz darauf kam mir ein anderes Auto entgegen. Ich kann nur erraten, was als Nächstes passiert ist. Mein Auto fuhr plötzlich nach links, überquerte die doppelte gelbe Trennlinie und fuhr direkt darauf zu. Hätte ich nicht schnell reagiert, um das Lenkrad in die entgegengesetzte Richtung zu reissen, hätte ich vielleicht seinen Weg gekreuzt» (4). Dabei hatte ja kein Mensch diesem Fahrer eine freihändige Spritztour empfohlen – wahrscheinlich auch Tesla nicht. Sondern natürlich hatte sich das Unternehmen abgesichert. «Was sagt das Handbuch?», fragte ein Videonutzer unter einem YouTube Filmchen eines anderen geschockten Tesla-Fahrers: «Achtung! Die automatische Steuerung ist eine hands-on-Funktion: Sie müssen immer die Hände am Lenkrad halten.»

Teslas Elektroautos: Entmündigung, horrende Preise, schlechte Leistung und kein Umweltschutz

Viele Kunden stehen Elon Musks Unternehmen Tesla misstrauisch gegenüber, was anhand der Unternehmensgeschichte nicht allzu unplausibel scheint: Neben den Milliarden an Staatshilfen, die Tesla erhält, baut das Unternehmen bekanntlich nur Elektroautos als Fortbewegungsmittel der Zukunft. Da Elektroautos von der internationalen Politik als Lösung für den vermeintlichen «menschgemachten Klimawandel» angeboten werden, verwundert es nicht, dass Musk mit der Politik einer Meinung ist und das Narrativ der Erderwärmung durch menschlich erzeugtes CO2 ebenfalls mantra-artig wiederholt. Dass es für diese Theorie keinerlei Beweise gibt, wurde bereits in der **ExpressZeitung Nr. 9/August 2017** erläutert.

Doch wie in der Ausgabe beschrieben: Selbst wenn es Beweise für die Theorie der menschgemachten Erderwärmung durch CO2 gäbe, sorgen Elektroautos nicht dafür, den CO2-Ausstoss zu verringern. Im Gegenteil: Ihre Energiebilanz steht mit dem Faktor 1,6 schlechter da als die eines Autos mit Verbrennungsmotor. Der Autor Edgar Gärtner schrieb: «Selbst in durchschnittlicher Ausführung und nicht überdimensioniert wie in Teslas Top-Modell verbraucht dessen Herstellung umgerechnet eine Energiemenge, mit der ein Auto mit Verbrennungsmotor über 30.000 Kilometer fahren könnte.»

Ein weiteres riesiges Problem ist die begrenzte Reichweite der elektrischen Autos: «Zwar gibt Tesla in seinen Verkaufsprospekten je nach Modell und Akku-Grösse inzwischen Reichweiten von 400 bis 600 Kilometern für eine Akku-Ladung an. Aber es liegt auf der Hand, dass solche Leistungen nicht an kalten Wintertagen erreichbar sind, weil dann die Heizung einen grossen Teil der Ladung beansprucht. Elektrische Kleinwagen schaffen an kalten Tagen nur etwa 60 Kilometer. Und dafür möchten wohl die meisten potenziellen Käufer keine 30.000 Euro hinblättern.»

So scheint Tesla hauptsächlich für zwei politische Ziele instrumentalisiert zu werden: Der legislativ erzwungenen Einführung von Elektrofahrzeugen und selbstfahrenden Autos. ***(tk)***

Das Auto reift beim Kunden

Nicht nur Software, sondern auch das Auto reift nämlich beim Kunden wie die berühmte Banane. Die Käufer werden einstweilen als Testfahrer eingespannt, die in Habachtstellung am Lenkrad sitzen müssen, um gegebenenfalls rechtzeitig einzugreifen und den Fehler anschliessend zu melden – von wegen «Fahrkomfort». Und wenn etwas schiefgeht, dann heisst es: Ihr Pech – haben Sie nicht die Bedienungsanleitung gelesen? **Die Bedienungsanleitungen fordern ausdrücklich, dass der verantwortliche Insasse das Fahrzeug überwacht, um jederzeit eingreifen zu können. Das heisst, dass man praktisch die ganze Zeit über die Hände am Lenkrad und die Füsse an den Pedalen haben muss, wie ein Fahrlehrer bei einem Fahranfänger. Ein solches Fahrzeug ist weder rechtlich noch technisch ein selbstfahrendes Vehikel, sondern höchstens ein Gefährt mit Fahrassistenzsystemen.** Genau das ist der Trick, mit dem derartige Fahrzeuge zurzeit überhaupt zugelassen werden: Dem Publikum gegenüber sprechen die Medien von «selbstfahrend», während der Wagen in Wirklichkeit auf Schritt und Tritt vom Fahrer überwacht werden muss. Da kann man natürlich auch gleich selbst steuern. Das ist schliesslich auch viel sicherer, als die ganze Zeit passiv zu warten, ob der Computer oder die Sensoren einen Fehler machen. Beim Fussball ist ein Feldspieler schliesslich auch viel mehr im Geschehen als ein Torwart, der nur manchmal eingreifen muss.

Keine Zeit zum Ausruhen: Bei Spurwechseln muss der Fahrer von LKWs im Autopilot die Hände schnell wieder am Lenkrad haben. Macht z.B. eine Sperrung einen Spurwechsel notwendig, muss manuell ins Lenkgeschehen eingegriffen werden.

Erkenntnis = Selbsterkenntnis

Funktionieren kann das selbstfahrende Auto deshalb nicht, weil vergessen wurde, dass Fahrzeuge dafür eine wichtige Fähigkeit brauchen: nämlich Kognition. Wenn man einmal alle Vorgänge und Fähigkeiten zusammenzählt, die beim Autofahren gebraucht werden, dann kommt man nicht umhin, zuzugeben, dass ohne Erkenntnis und Urteilsvermögen gar nichts geht. Um wirklich autonom fahren zu können, müssen Fahrzeuge ihre Umwelt begreifen und kognitiv erfassen, wie ein Mensch auch. Durchdenkt man beispielsweise den oben erwähnten Unfall, stellt man fest, dass man dafür lauter kognitive Begriffe benötigt:

Der Unfall eines auf «Autopilot» geschalteten Tesla in den USA zeigt, dass Teslas Software äusserst störanfällig ist und für Insassen noch ein grosses Risiko darstellt.

- So «erkannte» der Todes-Tesla zwar eine grosse, weisse Fläche – nicht aber, dass sich diese vor ihm bewegte und deshalb wohl kein Schild sein konnte.
- Die Abmessungen der Fläche hatte der Bordcomputer wohl auch nicht «begriffen», sonst wäre ihm «klar» gewesen, dass das Auto nicht unter dem Schild hindurchpassen würde.

Der Staat am Steuer

Daran sehen wir, dass ein solches Auto nicht ohne Kognition auskommt. Wirklich selbstfahrende Autos dürfen also nicht nur anhand einiger Sensoren reagieren (= Reflexe), sondern müssen das Gesamtbild begreifen, beurteilen und anschliessend reagieren (= Denken). Heute können sie die vielen Sensordaten aber noch nicht zu einem sinnvollen Bild zusammenfügen – und anschliessend «ein Urteil fällen» können sie schon gar nicht. Solange das nicht möglich ist, werden sie auch nicht sicher selbst fahren können, weil sie auf primitive «Wahrnehmungen» primitiv reagieren. Und selbst wenn: Die Frage ist natürlich, ob wir ein solches «erkenntnisfähiges» Auto überhaupt wollen – denn «Erkenntnis» heisst gleichzeitig natürlich auch «Selbsterkenntnis». Dann könnte ein solches Fahrzeug vielleicht auch ein eigenes Bewusstsein, eine eigene Identität, einen eigenen Willen und eigene Interessen entwickeln – verbunden mit all den Verwirrungen und Konflikten, die wir schon aus einschlägigen Science-Fiction-Romanen kennen. Denn diese Interessen müssen ja nicht unbedingt mit denen des Fahrers übereinstimmen. Wollen Sie in Zukunft also ernsthaft mit Ihrem Auto über das Fahrziel diskutieren? Wobei das ja noch nicht alles ist. Denn aufgrund der prinzipiell fehlerhaften Software müsste auch das «Auto-Ich» prinzipiell «gestört» sein. Wo ein Windows-Computer abstürzt, könnte ein solcher fahrbarer Untersatz womöglich «verrückt»spielen und Ausfälle, epileptische Anfälle oder Psychosen entwickeln. Fehlerbehaftete oder fehlprogrammierte Systeme, die autonom handeln können, können nun einmal immense Schäden anrichten. Wollen wir das wirklich? Und müssen wir dann den ADAC, den Psychiater oder ein Sondereinsatzkommando rufen? Erschaffen die Autohersteller hier etwa ein Frankenstein-Monster auf vier Rädern – den ersten wirklich autonomen (aber nicht fehlerfreien) Roboter? Egal: Politik und Industrie «fahren» plötzlich darauf «ab», als wäre das Ganze der lange gesuchte Stein der Weisen. **Das selbstfahrende Auto muss plötzlich her – koste es, was es wolle. Was beweist, dass es hierbei nicht um Fahrkomfort geht (der ist ohnehin trügerisch), sondern darum, schnellstmöglich eine Technologie zu entwickeln und unters Volk zu bringen, bei der – anders als bei bisherigen Autos – letztlich der Staat am Steuer sitzt.**

Googles Eric Schmidt: Alle deutschen Autos werden autonom fahren

Foto: guillaumepaumier.com, CC-BY.

Google-Verwaltungsratschef Eric Schmidt sieht eine grosse Zukunft für selbstfahrende Autos deutscher Hersteller. «Jedes deutsche Auto wird von einem Computer gesteuert werden», sagte Schmidt bei einem Auftritt auf der Gründerkonferenz NOAH in Berlin. Spätere Generationen würden lachen, wenn sie in alten Filmen sähen, wie sich Schauspieler hinters Steuer eines Autos setzten.

«Viele Aufgaben, in denen Computer inzwischen besser als Menschen sind, sollten auch von Computern erledigt werden», sagte Schmidt. Unter anderem machten sie keine für Menschen typischen Fehler.

Google arbeitet seit rund sechs Jahren an der Technologie für selbstfahrende Fahrzeuge und gilt damit als potenzieller Konkurrent auch für deutsche Hersteller. Die Autobauer haben in den vergangenen Jahren massiv in eigene Roboter-Wagen investiert. Die Branche erwartet, dass autonome Autos ab 2020 regulär im Strassenverkehr fahren werden.

Quelle: epochtimes.de, Googles Schmidt: Alle deutschen Autos werden autonom fahren, 10.06.2015

Anarchie auf Rädern

Denn schliesslich sind herkömmliche Kraftfahrzeuge nichts weiter als Werkzeuge der Anarchie, nicht wahr: Kaum sitzen wir am Lenkrad, fühlen wir uns frei und unbeobachtet und können überall hinfahren – wohin wir möchten. Früher sahen auch Politiker im Auto ein Verkehrsmittel der individuellen Freiheit. 1965 zum Beispiel sagte der damalige Verkehrsexperte der SPD, Helmut Schmidt: «Jeder Deutsche soll den Anspruch haben, sich einen eigenen Wagen zu kaufen» – und diesen natürlich selbst zu steuern, was denn sonst. «Das Auto symbolisiert Freiheit und Abenteuer», sagt der Psychoanalytiker Micha Hilgers: «Je mehr wir uns eingebunden fühlen, desto mehr suchen wir solche Nischen auf». [5]. **Aber Einsteigen, Anlassen und Losfahren, ohne irgendjemanden zu fragen – das geht ja gar nicht. Für den Staat hat das schliesslich den Nachteil, dass ein solches Fahrzeug schwer zu kontrollieren ist. Bei Bahn, Schiff und Flugzeug gibt es dagegen vorgeschriebene Wege und registrierte Tickets. Beim Auto aber nicht. Wenn der Fahrer das Pedal durchdrückt, kann er, wenn es dumm kommt, auf über 200 Kilometer pro Stunde beschleunigen und das Weite suchen. Ja, wer will denn so etwas? Der Staat jedenfalls nicht. Denn Freiheit, Unberechenbarkeit und Unabhängigkeit sind den Regierenden nun einmal suspekt.**

Tesla hat die NASA vorn...

Oder leide ich etwa unter Verfolgungswahn? Bestimmt. Denn mit dem Staat haben zum Beispiel Tesla und der Konzern von Elon Musk natürlich überhaupt nichts zu tun. Na gut: Bis auf die 4,9 Milliarden Dollar staatliche Subventionen vielleicht, die Musk für seine Unternehmen einstrich. Ausserdem zählte die Los Angeles Times «die günstige Arbeitskraft von Gefängnisinsassen» dazu, «mit der [der Musk-Konzern] Solarcity den deutschen Wettbewerber Solarworld für einen Staatsauftrag in Oregon ausstach – Teil eines Politskandals, der den dortigen langjährigen Gouverneur das Amt kostete» [6]. Schliesslich wären da noch rund 5,5 Milliarden Dollar Staatsaufträge von NASA und US-Luftwaffe an die Musk-Firma SpaceX: «Der jüngst erschienenen Musk-Biografie ist zu entnehmen, wie erleichtert der mit hohem Risiko agierende Unternehmer zu Weihnachten 2008 war, als die NASA überraschend 1,6 Milliarden Dollar für SpaceX ge-

Seite 39

währte – nachdem sie Musk kurz zuvor erlaubt hatte, zur Rettung von Tesla Geld von SpaceX zu leihen» (6). Wie praktisch: Geld von der NASA für Tesla über den Umweg SpaceX! Das Manager Magazin nannte Elon Musks Firmenkomplex deshalb sogar ein «Stasi-Imperium» – Pardon: «Staatshilfe-Imperium».

Nächster Halt: Polizeipräsidium

Ein anarchistisches Werkzeug wie das Auto erregt unausweichlich das Interesse der Behörden und ihrer Auftragnehmer aus der Industrie. Zwar können auch herkömmliche Autos schon kontrolliert und überwacht werden, zum Beispiel durch Kennzeichenleser an den Autobahnen oder durch Ortung der Handys ihrer Fahrer. Aber wer diese Überwachung partout nicht will, muss nur das Handy ausschalten und Landstrassen benutzen – schon ist er weg vom Überwachungsfenster. Jedenfalls in einem fahrbaren Untersatz des vergangenen Jahrhunderts. Aber viel besser wäre es natürlich, wenn man ein Fahrzeug nicht nur lückenlos überwachen, sondern auch von aussen steuern könnte: Verfolgungsjagden, Banküberfälle, Entführungen – alles wäre aussichtslos. Der Staat würde einfach einen Code benutzen, um sich in den Bordcomputer einzuklinken. Dort würde er ein neues Ziel einprogrammieren – sagen wir: «Polizeipräsidium» –, und das wäre es dann mit der Flucht. Ach ja: Die Türen würde er natürlich auch verriegeln.

Der türkische Präsident Erdogan beispielsweise hätte im Rahmen seiner Massenverhaftungen 2016 per Computerbefehl nur einige Zehntausend Fahrzeuge umprogrammieren müssen: Kaum wäre der Fahrer eingestiegen und hätte den Wagen gestartet, hätte der ihn «festgenommen» und zur nächsten Polizeistation gekarrt – oder ins nächste Geheimgefängnis, den nächsten Folterknast oder das nächste KZ. Der Fantasie sind da keine Grenzen gesetzt. Identifiziert hätte der Computer den Delinquenten über das Fingerabdruck-Zündschloss – ebenfalls eine praktische Erfindung für alle totalitären Systeme. Einen Zugriff auf den Bordcomputer vorausgesetzt, könnte man mit selbstfahrenden Autos auch unliebsame Personen beseitigen. Und dass die Dienste sich alle Mühe geben, solche «Hintertüren» in die Bordcomputer der von ihnen mitfinanzierten Fahrzeuge einzubauen, kann man sich vorstellen. Wenn der Delinquent unterwegs einen Unfall hat, ist das höchstens tragisch. Shit happens.

Teslas Elon Musk: Eines Tages wird es illegal sein, sein Auto selbst zu steuern

Da Elon Musk durch sein «Staatshilfe-Imperium» wohl auch mehr in die Politik verstrickt ist als manch anderer Unternehmer, könnte man die Worte, die er im März 2015 auf einer Technologie-Konferenz in San Jose äusserte als durchaus prophetisch interpretieren: «Die Menschen werden das Autofahren eines Tages verbieten, weil es gefährlich ist. [...] Eine Person kann keine Zwei-Tonnen-Todesmaschine fahren.»

Viele Beobachter interpretierten diese Äusserung weniger als neutrale Prognose, sondern mehr als Wunschvorstellung eines totalitären Technokraten. Deshalb sah sich Musk wenig später gezwungen, seine Aussagen auf Twitter zu relativieren. Er schrieb: «Um mich klar auszudrücken: Tesla ist klar dafür, dass Menschen erlaubt ist, ihre Autos zu fahren und wird dies auch immer sein. Das ist hoffentlich offensichtlich. [...] Jedoch wenn selbstfahrende Autos sicherer werden als vom Mensch gefahrene Autos, könnte die Öffentlichkeit letztere verbieten. Hoffentlich nicht.»

Nachdem er sich für die Zukunft eine Welt ohne manuell steuerbare Autos vorgestellt hatte, ruderte Elon Musk auf Twitter zurück und schrieb, Tesla unterstütze die Freiheit zwischen manuell und automatisch zu wählen. Doch reicht dieses Statement für eine saubere Weste? Letztendlich könnte der Staat, der ihn mit Milliardensummen unterstützt, dieses Verbot jederzeit durchsetzen. Würde das Musk nicht auch zum Komplizen dieser Grundrechtseinschränkung machen?

Ist das glaubwürdig? Schaden würde ein Verbot Tesla sicher nicht, denn so könnte die Öffentlichkeit dazu gezwungen werden, seine am freien Markt bisher noch unbeliebten Tesla-Modelle zu kaufen. ***(tk)***

Quelle: cnbc.com, Musk: Someday, driving a car will be illegal, 17.03.2015

Foto: RudolfSimon (https://commons.wikimedia.org/wiki/File:Angela_Merkel_and_Ulrich_Hackenberg.JPG) https://creativecommons.org/licenses/by-sa/3.0/deed.en

Angela Merkel: In 20 Jahren ist selbstständiges Autofahren verboten!

Aber das sind doch alles Horrorfantasien! Der Autor dieser Zeilen muss paranoid sein. Und ob: Zum Beispiel hatte ich die Vision, Bundeskanzlerin Angela Merkel habe gesagt, «wir werden in 20 Jahren nur noch mit Sondererlaubnis selbstständig Auto fahren dürfen». Der reine Irrsinn! Gerade als ich meine Pillen nehmen wollte, fiel mir ein, dass dies Wirklichkeit war. Merkel hatte das im Juni 2017 vor argentinischen Studenten geäussert. Ihre Begründung: «Wir sind das grösste Risiko.» Merkel sei von dem 15-stündigen Flug und dem Besuchsprogramm in Argentinien womöglich so müde gewesen, spekulierte die Website der Welt und von N24, dass ihr das wohl herausge-

rutscht sei (09.06.2017). Denn für eine Kanzlerin aus dem Land der Autobauer und -fahrer war dies schliesslich ein Satz wie ein Paukenschlag. Nur ein Echo hatte dieser Paukenschlag merkwürdigerweise nicht. Wer ihr oben genanntes Zitat im Juni 2017 bei Google eingab, fand es gerade einmal bei einer Handvoll Mainstream-Medien: auf der genannten Welt-Website und beim Münchner Merkur. Danach kamen bereits Fachmedien wie die Automobilwoche oder alternative Medien wie Golem, Politikforen oder reddit.com. Die Mehrheit der Medien beteiligte sich auch hier an einer Verschwörung des Schweigens.

Quellen:

1. futurezone.at, 28.05.2014
2. c-net, online, 25.09.2012
3. netzwelt.de, 23.08.2016
4. siehe YouTube-Video «Tesla Autopilot tried to kill me!», 15.10.2015
5. Die Zeit, online, 18.06.2003
6. Manager Magazin, online, 04.06.2015

Voreilig und schlampig: Bundesregierung erlässt Gesetzentwurf zur Zulassung automatisierter Fahrzeuge

Anscheinend kann es der Bundesregierung nicht schnell genug gehen: Anfang 2017 segnete sie einen Gesetzentwurf des Verkehrsministers Alexander Dobrindt zur Änderung des Strassenverkehrsgesetzes ab. Damit soll Deutschland das erste Land werden, auf dessen Strassen automatisiertes Fahren ohne Sondergenehmigung zulässig ist. «Das automatisierte Fahren ist die grösste Mobilitätsrevolution seit der Erfindung des Automobils», verlautbarte der Ex-Verkehrsminister. Und wem er mit der Gesetzesinitiative vor allem helfen wolle, machte er auch klar: Deutschlands Autokonzerne seien jetzt schon führend in dieser Technologie, und damit sie das im internationalen Wettbewerb auch bleiben, solle Deutschland zum «Leitmarkt» werden.

Die Bundesregierung will schleunigst automatisiertes Fahren auf deutschen Strassen zulassen, doch ihr Gesetzesentwurf verpflichtet den Fahrer dazu in bestimmten Situationen «unverzüglich» wieder selbst das Steuer zu übernehmen. Was dieses für die Klärung der Schuldfrage essenzielle «unverzüglich» bedeuten soll, wird in dem schlampigen Gesetzesentwurf nicht erläutert.

Doch in den Details ist dieser Gesetzentwurf sehr abenteuerlich und unreif: Zwar sollen Fahrzeuge mit hoch oder voll automatisierter Fahrfunktion danach auf unseren Strassen erlaubt sein, doch selbst wenn der Fahrer das Kommando an den Computer delegiert hat, bleibt die Verantwortung immer noch bei ihm oder dem Halter des Fahrzeugs. Vereinfacht ausgedrückt: Wenn es trotz Hightech kracht, zahlt erst mal die Versicherung des Fahrzeugbesitzers, und erst im Nachhinein wird geklärt, ob möglicherweise die Technik versagt hat und der Hersteller zahlt. Helfen soll dabei eine «Blackbox» im Auto, die genau aufzeichnet, was der Computer oder der Fahrer unmittelbar vor dem Unfall getan haben. Das kann im Einzelfall ziemlich interessant werden.

Ex-Verkehrsminister Dobrindt schwadronierte schon über den Vorteil automatisierter Systeme: «Wir ermöglichen damit, dass der Fahrer während der automatisierten Fahrt die Hände vom Lenkrad nehmen darf, um etwa im Internet zu surfen oder E-Mails zu checken.» Praktisch wäre das ja, sofern die Systeme wirklich zuverlässiger funktionierten als etwa bei dem tödlichen Unfall eines auf «Autopilot» geschalteten Tesla vergangenes Jahr in den USA.

Doch der Ex-Verkehrsminister scheint seinen eigenen Gesetzentwurf nicht genau gelesen zu haben. Dort steht nämlich, dass der Fahrer, etwa wenn ihn das System dazu auffordert, «unverzüglich» wieder selbst das Steuer übernehmen muss. Was aber bedeutet «unverzüglich»? Versuche mit Fahrsimulatoren haben gezeigt, dass es mindestens fünfzehn Sekunden dauert, bis ein mit anderen Dingen beschäftigter Fahrer wieder die aktuelle Fahrsituation vollständig erfasst. In der Regel hat es dann aber schon gekracht. Meist geht es nur um Sekundenbruchteile. Wer würde dann die Schuld an einem Unfall tragen? Der Fahrer oder die Technik? Und wären die Autohersteller verpflichtet, in diesen Fällen immer zu haften?

Träte der Gesetzentwurf in der momentanen Fassung in Kraft, wäre es für den Fahrer sicher keine gute Idee, sich mit Lesen oder Surfen zu beschäftigen, während der Bordcomputer lenkt. Wenn man das Gesetz wörtlich nimmt, blieben die Vorteile der neuen Technik grösstenteils auf der Strecke, weil der Fahrer eben nicht auf die Technik verweisen könnte. Eine Präzisierung wäre dringend nötig. U.a. deshalb fand Dobrindts Entwurf wenig Zustimmung bei den Experten des Verkehrsgerichtstages, dessen Präsident Kay Nehm die «völlig unangebrachte Hast» der Bundesregierung kritisierte. Weiterhin blieben ethische Fragen, etwa die, wie der Computer sich im Dilemma zwischen zwei Übeln entscheidet – z.B. an die Wand fahren oder Radfahrer überfahren? –, im Gesetz aussen vor. Der Minister mogele sich um die wirklich harten Fragen herum.

Für den Bundesrat war der Entwurf ebenfalls noch zu unausgereift. Er bilde «keine ausreichende Grundlage für die rechtlich sichere wie auch wirtschaftliche Nutzung der Technologie», heisst es in der Stellungnahme. Der Fahrer würde zu grossen Risiken ausgesetzt. Nötig seien klarere Definitionen.

Quelle: zeit.de, Entschieden unscharf, 16.02.2017

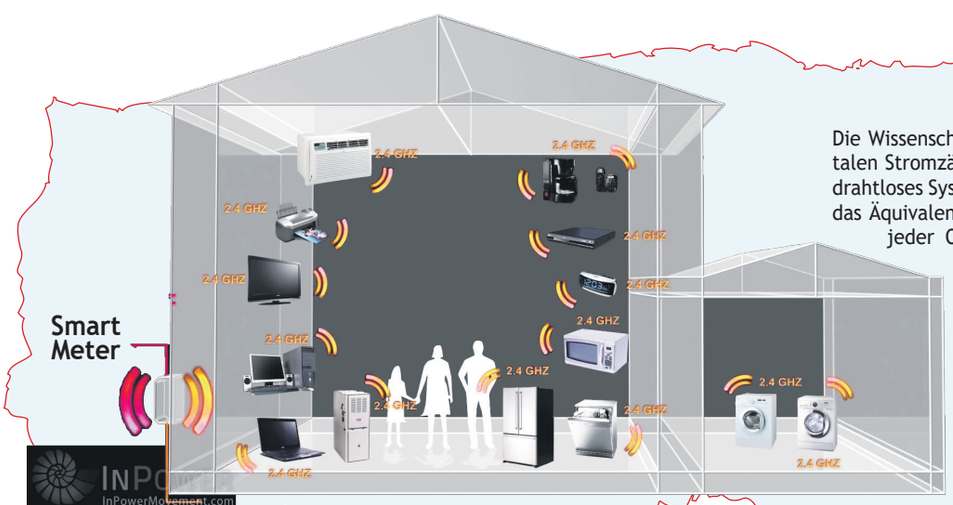
Smart Meter

Dauerüberwachung durch das digitale Stromnetz?

Ein intelligenter Stromzähler (Smart Meter) ist ein kleines, digitales Gerät, das aussen am Haus eines Stromkunden installiert wird. Im Gegensatz zu den ausgedienten analogen Stromzählern, die inzwischen weltweit durch die neuen digitalen Modelle ersetzt werden, ist ein Smart Meter in der Lage, nicht allein den Stromverbrauch zu messen, sondern die genaue Stromnutzung innerhalb eines Hauses detailliert aufzuzeichnen. Jedes Mal, wenn jemand das Licht oder ein Gerät anschaltet, wird ein spezifischer Code übertragen, der dann durch den intelligenten Zähler ans Netz und den Stromanbieter übermittelt wird.

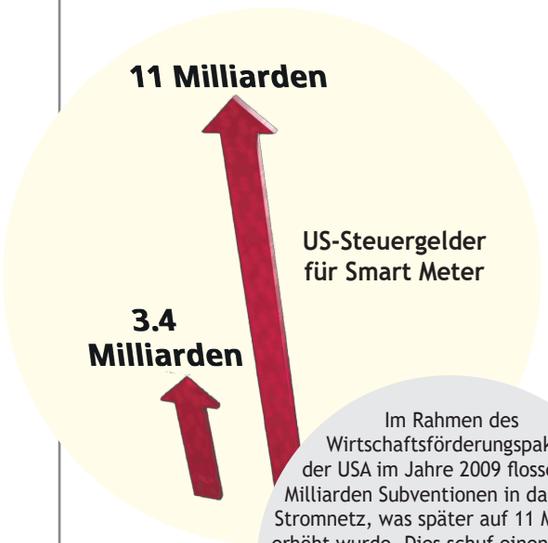
Die «Smart»-Stromnetze bieten laut den Stromversorgern viele Vorteile: verbesserte Energiesicherheit, Reduzierung der Treibhausgase, Verbesserung der städtischen Luftqualität und optimierte Netzauslastung. Doch von den Schattenseiten wird selten gesprochen: Mit den neuen Smart Metern können Stromkonzerne die Aktivitäten ihrer Kunden nachvollziehen und analysieren. Die Daten der Smart Meter geben viel über das Privatleben der Stromkunden preis. So könnte das Überwachungspotenzial der digitalen Stromzähler von der Regierung noch weiter ausgereizt werden, denn sollte sich z.B. die internationale Klimapolitik zur Beschränkung des CO_2-Ausstosses weiter verschärfen, könnten Stromkunden bald Mahnungen drohen wie «Sie haben Ihr Stromgerät XY in diesem Monat 14 Stunden zu lange laufen lassen. Bitte schränken Sie dessen Nutzung ein.»

Theoretisch müsste um die Stromreduzierung nicht einmal gebeten werden, denn die neuen Zähler können sowohl senden als auch empfangen. D.h. sie könnten den Stromkonzernen oder der Regierung erlauben, jedes Gerät in Ihrem Haus nicht nur zu überwachen, sondern auch zu steuern. Ein Gerät, das von dem Kunden nach Meinung der Anbieter zu oft benutzt würde, könnte dann einfach abgeschaltet werden, ohne überhaupt mit dem Kunden in Kontakt treten zu müssen. Mit diesen technischen Fähigkeiten könnten Smart Meter eine essenzielle Rolle bei der Errichtung einer Welt spielen, in der Menschen unter ständiger Beobachtung stehen würden.



Die Wissenschaftsjournalistin Blake Levitt sagt über die digitalen Stromzähler: «Die Definition eines Smart-Netzes ist ein drahtloses System, das im Prinzip jedes Gerät in Ihrem Haus in das Äquivalent eines Handys verwandelt. Das bedeutet, dass jeder Ofen, jede Klimaanlage, jede Kaffeemaschine, jeder Drucker, jedes einzelne Haushaltsgerät eine Antenne eingebaut haben wird, die Ihre Verbrauchsdaten an einen intelligenten Zähler weitergeben wird, der dann wiederum Ihre Verbrauchsdaten an einen Sendemast überträgt, der die Information zum Stromversorger weiterleitet. Angeblich zum Zweck der Rechnungsstellung.»

Steuergelder aus aller Welt, vor allem aus den USA, sind zu einigen der grössten Konzerne der Welt geflossen, um möglichst viele Stromkunden möglichst schnell mit einem Smart Meter zu versorgen. General Electric zum Beispiel ist der grösste Hersteller von Smart Metern. Sie werden in China produziert. Das zeigt, dass viele Regierungen ein grosses Interesse an der Implementierung dieser Technologie haben.



Im Rahmen des Wirtschaftsförderungspakets der USA im Jahre 2009 flossen 3,4 Milliarden Subventionen in das Smart-Stromnetz, was später auf 11 Milliarden erhöht wurde. Dies schuf einen massiven finanziellen Anreiz für die Stromversorger, sich an dem Programm zu beteiligen. Und wegen der Subventionen waren die Stromversorger verpflichtet, eine gewisse Anzahl dieser Stromzähler zu installieren.

would give us real-time feedback and control over our energy use. He basically wanted to merge the grid with the Internet so we could adjust our air conditioners with our iPhones when we were out of the house, program our appliances to save us energy and money and sell power from solar panels and electric cars back to our utilities.

After the election, Obama wanted his economic stimulus package to include some iconic, futuristic legacy projects to advance his long-term agenda. The smart grid seemed perfect, a modern moon mission, a 21st century version of the interstates. He suggested pouring in $100 billion. "Let's just build it!" he told his transition team. His aides explained that that wasn't possible or even desirable. Utilities own the grid, and they could pay to upgrade it themselves. But it would take decades to convert an analog grid to digital and string high-voltage wires nationwide. Ultimately, Obama settled for $[illegible] billion in seed money. "There was this sense of frustration," his former budget director Peter Orszag recalled when I interviewed him for my forthcoming book on the stimulus. *The New New Deal: The Hidden Story of Change in the Obama Era*. "Here's

Laut Time Magazine, schlug Präsident Obama vor, 100 Milliarden Dollar in ein Smart-Stromnetz zu investieren, mitten in einer Wirtschaftskrise, direkt nach der Wahl im Jahr 2008. Laut Wikipedia war der Hauptgrund für diese beispiellose Zuwendung von öffentlichen Geldern die letztendliche Reduzierung des Energieverbrauchs um mindestens 4%.

Keine Energieeinsparung durch Smart Meter! Was ist dann der Zweck?

BBC News Sport Weather Travel Culture Autos

NEWS UK POLITICS

Home | US & Canada | Latin America | UK | Africa | Asia | Europe | Mid-East | Business | Health | Sci/Environment | Tech | Entertainment | Video

England | Northern Ireland | Scotland | Wales | UK Politics | Education

15 May 2013 Last updated at 10:00 ET

163 Share

Smart meters 'a waste of money', MPs told

The plan to introduce smart meters into every home across Britain is a "waste of money", MPs have been told.

The units are designed to show people exactly how much energy they are using at any time, but the project has been delayed by a year because of problems.

Energy analyst Alex Henney said people could be given live information on their energy use via weblinks or smartphone apps much more

At White H
David Bec
Pope Franc
Space life

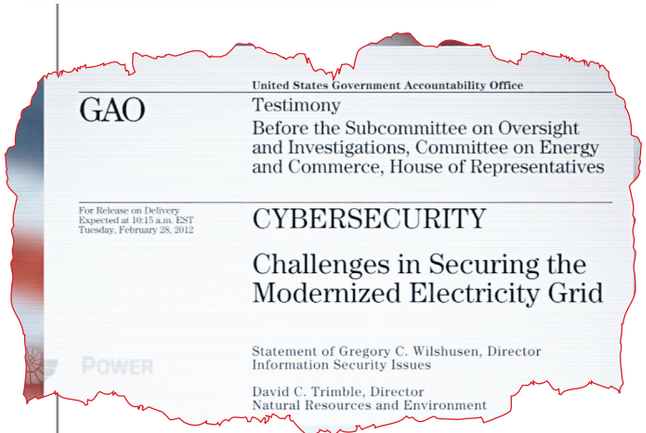
File not

Reale Verbrauchsdaten zeigen jedoch, dass die Installation von intelligenten Zählern nicht die geringste Energieeinsparung produziert. Ein Bericht für «Illinois Public Utilities» zeigte keinerlei statistischen Unterschied in den Resultaten. Darüber hinaus gehen Smart Meter auch schneller kaputt als analoge Zähler.

Mehr Sicherheit? Ehemaliger CIA-Direktor warnt vor Hacker-Attacke auf Smart-Stromnetz

James Woolsey, ehemaliger CIA-Direktor, warnte bereits vor den Gefahren eines digitalen Stromnetzes: «Die bauen jetzt ein sogenanntes ‚intelligentes Stromnetz'. Damit wird es viel einfacher, per Handy mit zu Hause zu kommunizieren, und an einem heissen Nachmittag die Klimaanlage anzuschalten, auch wenn man nicht zu Hause ist. Super. Aber das könnte doch auch bedeuten, dass ein Hacker in Shanghai mit seinem Handy das Gleiche oder etwas Schlimmeres tun könnte. Und ein sogenanntes ‚Smart'-Stromnetz, das so störanfällig ist wie unseres, ist überhaupt nicht intelligent. In Wahrheit ist es ein dummes Netz.»

Auch David Chalk, Hacking & Cyber-Experte, versteht nicht, wie Regierung und Stromkonzerne den Kunden eine sicherere Stromversorgung versprechen können: «Die Störanfälligkeit des Internets wird jetzt auf die Stromnetze übertragen. Ohne eine hundertprozentige Garantie, dass die Verbindung über Internet oder drahtlose Kommunikation sicher ist. Wir laufen Risiko, den Strom, der diese Nation am Leben hält, verwundbar zu machen.»


United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:15 a.m. EST
Tuesday, February 28, 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

Statement of Gregory C. Wilshusen, Director
Information Security Issues

David C. Trimble, Director
Natural Resources and Environment

Sogar die US-Regierung gibt in einem ihrer Dokumente zu, dass ein Smart-Stromnetz die Tür für Cyber-Terrorismus in riesigem Ausmass öffnet.

Kalifornien, Vereinigte Staaten:

Gemeinden, die sich gegen Smart Meter wehren: **57**

und es werden immer mehr

Installationen gegen den Willen der Kunden

Trotz massenhafter Proteste wird der undemokratische Prozess der latenten Installation von intelligenten Zählern überall in den USA nach dem gleichen Muster durchgesetzt. John Horgan, Energie-Kritiker von der Neuen Demokratischen Partei (NDP) aus Kanada kommentiert: «Ich möchte nicht unbedingt das Wort ‚Faschismus' benutzen. Geschichtlich betrachtet, sind wir noch nicht soweit. Aber ‚Korpokratie', also Herrschaft der Grosskonzerne, ist eine passende Bezeichnung.»
Wie kann es sein, dass die Unternehmen, die das globale Smart-Stromnetz verwirklichen wollen, ihre Pläne einfach durchdrücken trotz einer langen Liste potentiell katastrophaler Nachteile?

Verfolgung auf Schritt und Tritt durch den Stromzähler

Ian R. Crane, geopolitischer Forscher aus Grossbritannien, sagt: «Hauptziel des Planes ist es, jede Bewegung innerhalb eines Hauses nachvollziehbar zu machen. Jedes Mal, wenn jemand das Licht oder ein Gerät anschaltet, übertragen diese einen spezifischen Code, der dann durch den intelligenten Zähler ans Netz übermittelt wird. Daher kann jeder, der das möchte, einen bestimmten Haushalt auswählen und genau verfolgen, was dort vor sich geht.»

theguardian | TheObserver

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | Tech | TV | Video

Environment › Energy monitoring

Energy smart meters are a threat to privacy, says watchdog

European Data Protection Supervisor warns 'massive collection of personal data' could be accessed without safeguards

Jamie Doward and Caroline Mortimer
The Observer, Sunday 1 July 2012

Share
Tweet this
+1 11
Share 4
Email

Article history

Environment
Energy monitoring
Energy efficiency · Energy

World news
Privacy

Genaues Verbrauchsprofil für jedes Individuum

James S. Turner, Menschenrechtsanwalt aus Washington D.C., meint: «So kann man sehen, wann der Kühlschrank benutzt wird, wann der Fernseher an ist und was Sie mit Ihrer Energie tun. So lässt sich für jedes Individuum ein genaues Verbrauchsprofil erstellen.»

Congressional Research Service

Smart Meter Data: Privacy and Cybersecurity

Brandon J. Murrill
Legislative Attorney

Edward C. Liu
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

February 3, 2012

Verstoss gegen das Recht auf Privatsphäre

Ein Forschungsbericht des US-Kongresses kam zu dem Schluss, dass intelligente Stromzähler in den USA eine Verletzung des vierten Zusatzartikels zur Verfassung darstellen. Der Bericht sagt: «Zentraler Punkt des Vierten Zusatzartikels ist das Recht eines Menschen, sich in sein Heim zurückzuziehen, und dort frei von unverhältnismässigen Regierungseinflüssen zu verbleiben. […] Mit intelligenten Zählern wird die Polizei Zugang zu Daten haben, die es erlauben, den Tagesablauf der Bewohner genau zu verfolgen, wie zum Beispiel ihre Ess-, Schlaf- und Duschgewohnheiten; welche Geräte sie wann benutzen, und ob sie lieber fernsehen als auf dem Heimtrainer zu trainieren, und vieles mehr.»

Kalifornische Stromversorger geben Weitergabe der Daten an Dritte zu, sprechen jedoch im gleichen Atemzug von «Geheimhaltung»

Smart Energy Portal .NET

SHARE Print

California Commission Adopts Rules to Protect the Privacy and Security of Customer Electricity Usage Data

Topics News, Advanced Metering, State, Energy Delivery, Smart Grid, Policy

July 31, 2011 | By Nikki Chandler

The California Public Utilities Commission, as part of its efforts to build a smart grid for California, unanimously approved rules to protect the privacy and security of customer usage data generated by smart meters.

The decision applies to Pacific Gas and Electric Co., Southern California Edison, San Diego Gas and Electric Co., the companies that assist utilities in their operations, companies under contract with the utilities, and other companies that, after authorization by a customer or by the action of the CPUC, gain access to a customer's usage data directly from a utility.

In addition to the adopted rules protecting the privacy and security of usage data, the decision requires utilities

Eine Pressemitteilung von 2011 mit dem Titel «Die Kalifornische Kommission der Stromversorger verabschiedet Regeln zum Schutz der Privatsphäre und Datensicherheit» verkündete Folgendes: «Unsere heutige Entscheidung wird die Geheimhaltung und Sicherheit der Stromverbrauchsdaten unserer Kunden gewährleisten und gleichzeitig autorisierten Dritten erlauben, diese Informationen zu nutzen.»

Kommissionsmitglied Timothy Alan Simon fügte hinzu: «Ich befürworte die heutige Entscheidung, weil sie Verbrauchern und Dritten den Zugang zu Stromverbrauchsinformationen erleichtert. […] Ich hoffe, diese Entscheidung wird das Marktinteresse stimulieren.»

Stromdaten werden heute schon verkauft

Und während viele Stromversorger immer noch behaupten, dass sie diese Daten sicher verwahren werden, zeichnet sich langsam ein neues Bild ab: «Hier in Kalifornien verkaufen die Stromversorger unsere privaten Stromverbrauchsdaten gegen Profit an Dritte. Anstatt diese Praxis zu verurteilen, hat die California Public Utilities Commission sie gefördert», so Joshua Hart, Direktor von Stopsmartmeters.org.

San Francisco Chronicle

Thursday June 20, 2013

Home Local US & World Sports Biz & Tech Opinion Food A&E Lifestyle

SURVEILLANCE

Is your smart meter spying on you?

By David R. Baker

Phone records and e-mail aren't the only kinds of personal data that government agencies can collect on Americans. They can look at your home's energy use, too. And that information can be revealing. California's electric utilities last year disclosed the energy-use records and other personal information of thousands of customers, according to reports the companies filed with state regulators.

Golden Gate Park trees 'decapitated'

Black market run by recycling

By Vivian Ho

Im Sommer 2013 wurden diese neuen Intentionen noch deutlicher. Der San Francisco Chronicle offenbarte, dass Kaliforniens Stromversorger die Stromverbrauchsdaten und andere persönliche Informationen von tausenden Kunden an Behörden der US-Regierung weitergegeben hatten.

Getty

Smart grid powers up privacy worries

By DAVID PERERA | 1/1/15 9:00 AM EDT

The next Big Data threat to our privacy may come from the electricity we consume in our homes.

"Smart" online power meters are tracking energy use — and that data may soon be worth more than the electricity they distribute.

Anfang 2015 gab ein Aufsichtsratmitglied eines Stromversorgers zu, dass von Stromzählern gesammelte Haushaltsüberwachungsdaten wesentlich mehr wert sind als der Strom selbst.

Stromanbieter kooperiert zur Auswertung von Daten mit US-Regierung

Stephen Pratt, technischer Direktor von Centerpoint Energy, einem Hersteller von Smart Metern, sagte: «Vor sechs Jahren waren intelligente Zähler noch ziemlich selten. Heute haben 60 Millionen Konsumenten Zugang zu Information darüber, wie viel Energie wir benutzen. Wie wir sie benutzen. Wann wir sie benutzen. Und das Spannendste daran ist für mich, dass wir eine ganze Organisation haben, die versteht, dass Daten ein Wirtschaftsgut sind, zum ersten Mal in der Geschichte unseres Unternehmens. Und wir haben eine Menge Daten. Wir vollziehen 221 Millionen Zählerablesungen pro Tag, was täglich ungefähr ein Terrabyte Daten produziert. Wir können diese Daten auswerten. Centerpoint Energy […] arbeitet mit mehreren Regierungsbehörden, um sicherzustellen, dass wir gut positioniert sind.»

Ex-CIA-Direktor räumt Überwachung durch Haushaltsgeräte ein

DANGER ROOM

WHAT'S NEXT IN NATIONAL SECURITY

PREVIOUS POST NEXT POST

CIA Chief: We'll Spy on You Through Your Dishwasher

By Spencer Ackerman March 15, 2012 | 5:35 pm | Categories: Info War, Spies, Secrecy and Surveillance

Follow @attackerman

More and more personal and household devices are connecting to the internet, from your television to your car navigation systems to your light switches. CIA Director David Petraeus cannot *wait* to spy on you through them.

...arlier this month, Petraeus mused about the emergence of an "Internet of Things" — that is, wired ... a summit fo... Tel, the CIA's venture capital firm. "'Tr... ...al' is an overused ... ...allies to these technologies," Pet...

WIRED, March 2012

David Howell Petraeus war von 2011 bis 2012 Direktor der CIA und zuvor Offizier der US-Armee, zuletzt im Dienstgrad eines Vier-Sterne-Generals. 2012 gestand er unverhohlen: «Täuschen Sie sich nicht. Wir haben die Möglichkeit, Ihre Haushalte durch Ihre Geräte zu überwachen. Und wenn wir die Möglichkeit haben, dann werden wir sie wahrscheinlich auch nutzen.»

Ehemaliger NSA-Mitarbeiter: «Permanenter, universeller Lauschangriff auf jede Person»

Thomas A. Drake, ehem. Leitender Angestellter bei der Nationalen Sicherheitsverwaltung der USA (NSA) sagt: «Wir sehen hier den Aufbau einer Überwachungsgesellschaft. Und wir sehen den Aufbau eines Überwachungsnetzes. Damit erhebt sich das Gespenst einer sanften Tyrannei. Das Gespenst von: ‚Sie sind automatisch verdächtig, bis Sie beweisen, dass Sie es nicht sind.' Das Gespenst eines universellen Lauschangriffs auf die Bürger. Ein permanenter universeller Lauschangriff auf jede einzelne Person, den man nach Belieben aktivieren kann. Was passiert, wenn sie Sie nicht mögen? Was passiert, wenn Sie sich kritisch gegenüber der Regierung äussern? Was passiert, wenn Sie etwas sagen, das man als ‚unloyal' betrachten könnte? Also, das ist nicht mehr das Land, das ich viermal in meiner Regierungskarriere zu verteidigen geschworen habe.»

«Die Kontroll-Elite versucht, eine globale bargeldlose Währung zu schaffen und sie plant das auf der Basis von Emissionszertifikaten. Das bedeutet, Ihr Energieverbrauch könnte je nach Ihrem Verhalten zugeteilt werden. Und sie will es kontrollieren. Diese Zähler, die jetzt installiert werden, die sowohl senden, als auch empfangen können, würden ihnen erlauben jedes Gerät in ihrem Haus nicht nur zu überwachen, sondern auch zu steuern. Wieso glauben die Regierungen eigentlich, dass sie uns einen totalitären Staat aufzwingen können? Ohne dass wir es überhaupt bemerken!», so Foster Gamble, Regisseur des Films «Thrive».

Hol Dir Deine Macht zurück 2017 - offizieller Film

74.635 Aufrufe 945 54 TEILEN

Jo Conrad
Am 28.12.2017 veröffentlicht

ABONNIEREN 15 TSD.

Die Bilder und Texte dieses Artikels basieren auf der Dokumentation «Hol dir deine Macht zurück» – eine Übersetzung des amerikanischen Films «Take back your Power». Dieser Dokumentarfilm über Smart Meter zeigt die augenöffnende Geschichte, die hinter dem Smart-Netz liegt. Mit 20% neuen Inhalts deckt dieser bündige 83-minütige Film sowohl schockierende Fakten als auch Beweise aus erster Hand bezüglich Überwachung, Korruption, hochschiessender Rechnungen, gefährlicher Anfälligkeit, Erpressung und sogar tausenden von Hausbränden und Explosionen auf. Die fesselnde, gerade rechtzeitige Untersuchung führt zum beunruhigenden Schluss, dass Versorgungsunternehmen und Regierungen gefährliche Überwachungsmechanismen einsetzen, um uns alle in den eigenen vier Wänden auszuspionieren — und das ohne unsere Zustimmung.

Mehr Informationen auf den Webseiten:
Stop-smartmeter.at und InPowerMovement.com

BEWUSST.TV
DER BILDUNGSKANAL

Die deutsche Version des Filmes wurde von der Webseite bewusst.tv des Journalisten Jo Conrad zuerst veröffentlicht. Auf bewusst.tv ist darüber hinaus ein Interview mit dem Filmemacher Josh Del Sol zu sehen: bewusst.tv, Hol Dir Deine Macht zurück – Smartmeter adé, 28.12.2017

von Gerhard Wisnewski

Rauchmelder: Die Wanzen an der Zimmerdecke

- Moderne Rauchmelder, deren Installation in deutschen Wohnungen inzwischen verpflichtend ist, haben das technische Potenzial, als Allzweck-Überwachungsgerät zu dienen. Die neuen Modelle verfügen über eine Funkverbindung nach aussen, ein Ultraschall-Mikrofon und einen Mikrochip.
- Mit der Ultraschall-Technik wäre es theoretisch sogar möglich herauszufinden, ob der Mieter gerade nicht zu Hause ist oder ob sich in den Räumen etwas bewegt. Es soll nicht behauptet werden, dass dies schon stattfindet, aber egal ob Staatsmacht oder elektronikbegabte Hacker: Sie finden in Ihrer Wohnung bereits eine grosszügig gestaltete Technikplattform vor, die man entsprechend manipulieren oder austauschen kann.
- Das Ableseunternehmen ista erhält seine Daten von Rauchmeldern, Heizkostenverteilern, Wärme- und Wasserzählern usw. bereits zunehmend digital durch Funk aus deutschen Wohnungen. Von Jahr zu Jahr wird die Technik der Ablesegeräte weiter digitalisiert. Kommen noch die Daten der «intelligenten Stromzähler» (Smart Meter, siehe S. 42) hinzu, braucht man fast schon keine Überwachungskamera mehr, um unsere Aktivitäten zu beobachten, denn anhand des Stromverbrauchs zu bestimmten Tages- und Nachtzeiten lässt sich sehr genau ablesen, was in einer Wohnung passiert.
- Das technische Potenzial der neuen Rauchmelder könnte auch bald im Rahmen des «Smart Homes» (siehe S. 51) zum Tragen kommen, indem man den Rauchmelder zum Multifunktionsgerät umbaut, das neben Rauch auch Bewegung, Helligkeit oder Temperatur registriert.

Was würden Sie sagen, wenn man Ihnen einen Technikträger in die Wohnung setzen würde, in den Sie nicht hineinschauen dürfen, den Sie nicht selbst ein- oder ausschalten dürfen und der eine Funkverbindung nach aussen sowie eine Stromversorgung für mehrere Jahre besitzt? Mit anderen Worten: eine vollkommen autarke, verplombte Hightech-Plattform, in die man im Prinzip alles einbauen kann, was man will, auch Mikrofone und Kameras, ohne dass Sie irgendetwas dagegen tun können? Also eine technische No-go-Area und eine Allzweck-Überwachungswaffe in Ihrem Wohnzimmer, in Ihrem Schlafzimmer und in Ihrem Kinderzimmer? Das käme gar nicht infrage, meinen Sie? Oh doch – es ist bereits millionenfach geschehen, und es passiert auch jetzt noch jeden Tag.

Das ist Ihnen gar nicht aufgefallen? Mir auch nicht. Und zwar, weil man diesen Technikträgern einen harmlosen Namen gegeben hat. Oder besser: sogar einen euphemistischen, nützlich klingenden Namen. Und dieser Name lautet «Rauchmelder». Der ist natürlich in jeder Wohnung ein Muss, schliesslich toben doch jedes Jahr regelrechte Feuerstürme übers Land, denen Zehntausende Menschen zum Opfer fallen, oder nicht? Na ja – eigentlich nicht. Gemessen an den anderen Todesursachen ist ein Feuertod eine der unwahrscheinlichsten Todesursachen überhaupt, übertroffen zum Beispiel noch von einer Pilzvergiftung und einem Blitzschlag. Zudem ist die Schutzwirkung der Rauchmelder statistisch nicht bewiesen. Daten, wie viele Menschenleben Rauchmelder in Deutschland bereits gerettet haben, gibt es nicht. Vergleicht man die Zahl der Brandtoten in Bundesländern mit und ohne Installationspflicht, «so fällt auf, dass nichts auffällt», schrieb die Wirtschaftswoche am 14. November 2012. Und ausgerechnet in dem Raum, in dem die meisten Brände entstehen, darf der Rauchmelder nicht installiert werden: in der Küche. Bis 2020 müssen offenbar aufgrund erfolgreicher Lobby-Arbeit praktisch überall im Bundesgebiet Brandmelder eingebaut sein. Besonders die Elektroindustrie scheint einen besonders guten Draht nach Berlin und Brüssel zu haben, wird sie doch mit grosszügigsten Konjunkturprogrammen wie der «Energiesparlampe», dem Elektroauto und nun den High-Tech-Rauchmeldern verwöhnt.

Unidentified Spying Object?

Betrachtet man beispielsweise einen Rauchmelder der Firma ista, kommt man aus dem Staunen gar nicht mehr heraus: Was will der eigentlich wirklich an meiner Wohnzimmerdecke?

Im Einzelnen besitzt er nämlich

- eine höhere mechanische Stabilität,
- eine Resistenz gegenüber Luftfeuchtigkeit, Temperaturschwankungen und elektromagnetischen Störungen (Handys und WLAN)
- einen Schutz vor dem Eindringen von Fremdkörpern in die Messkammer
- eine Verstopfungserkennung: «Anhand von Messungen der Luftzirkulation im Gerät wird eine Verstopfung der Raucheintrittsöffnungen präzise erkannt» – aber natürlich auch ein Klebeband, mit dem der Bewohner versuchen könnte, sich wie bei einer Laptop-Kamera gegen eine mögliche Beobachtung zu schützen
- eine Demontageerkennung: Ein Abbau «wird sowohl am Gerät als auch am Montagesockel sofort erkannt» – eine Demontage durch den Wohnungsbesitzer oder Bewohner ist also nicht ohne Weiteres möglich
- eine mechanische Plombe zur Vorbeugung gegen «Demontagen», «Manipulation» und «Diebstahl»
- ein Batteriemanagement: «Die Batteriekapazität ist für eine Laufzeit von zehn Jahren ausgelegt und wird regelmässig automatisiert geprüft» (das Gerät arbeitet für zehn Jahre vollkommen autark)
- eine stumme Alarmprüfung: «Der Alarmgeber wird regelmässig durch eine lautlose Schwingungsmessung auf seine Funktionsbereitschaft geprüft»
- eine Funkverbindung nach draussen [1]

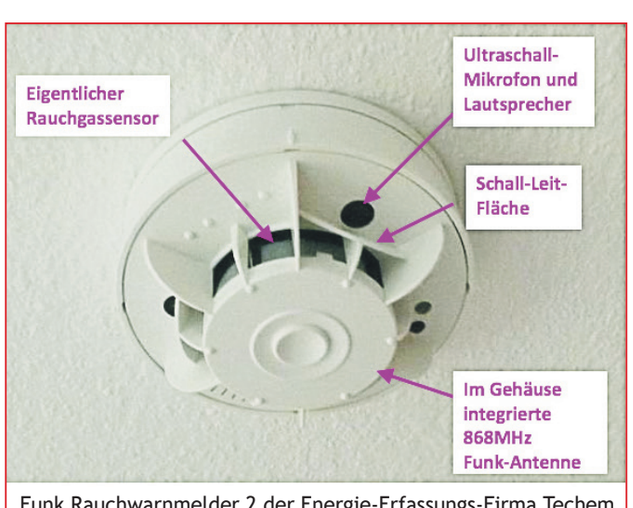
Seite 47

Ein ziemlicher Aufwand für einen einfachen «Rauchmelder», finden Sie nicht auch? Wofür braucht das Gerät all die aufgeführten Funktionen? Und was gibt es zu verbergen? Der «Rauchmelder» erscheint wie ein «Hochsicherheitstrakt», der vor allem vor demjenigen geschützt werden soll, den es angeblich zu schützen gilt – nämlich den Bewohner der Wohnung oder des Hauses.

Abhörwanze mit Funkübertragung

Es kommt aber noch besser. Schon am 10. Dezember 2014 veröffentlichte der Messingenieur Bernd Laquai eine ausführliche Analyse des «Funkrauchwarnmelders 2», der zum Beispiel von der Firma Techem verbaut wird. Auch Techem macht sich offenbar extreme Sorgen, ob der Rauchmelder wirklich freie «Sicht» auf den Wohnraum hat. **So hat dieser Rauchmelder noch einige sehr spezielle Eigenschaften. Statt per Messung der Luftzirkulation im Inneren, überwacht dieses Gerät sein Umfeld mithilfe von Ultraschall – wie eine Fledermaus.**

Die Ultraschall-Transceiver «enthalten eine dünne Piezokeramik-Scheibe, die sowohl als Lautsprecher wie auch als Mikrofon arbeitet», so Laquai. Genauso kann der Schallwandler im Missbrauchsfall «auch als normales Mikrofon im hörbaren Bereich arbeiten. Bei diesen Frequenzen ist die Empfindlichkeit sicher nicht maximal, aber aus der Verfügbarkeit anderer Mikrofontypen mit Piezo-Schallwandler in kleinsten Bauformen wird schnell klar, dass sich damit auch Sprache in elektrische Signale umwandeln lässt. Wenn auch nicht die übrige Ansteuerelektronik auf der Platine für die Digitalisierung von Sprachsignalen vorgesehen ist, so ist diese Funktionsweise durch Manipulation mit hinzugefügten Komponenten durchaus möglich. Daher kann nicht ausgeschlossen werden, dass ein äusserlich normal erscheinender Funkrauchwarnmelder 2 nach entsprechender Manipulation auch als Abhörwanze mit Funkübertragung verwendet wird.» Im Missbrauchsfall, wohlgemerkt.



Funk Rauchwarnmelder 2 der Energie-Erfassungs-Firma Techem

Der «Funkrauchwarnmelder 2» der Firma Techem könnte mit seiner Ultraschall-Technik Sprache in elektrische Signale umwandeln und damit als Wanze dienen. Es wäre durch das Aussenden von Ultraschallwellen theoretisch sogar möglich, herauszufinden, ob sich in den Räumen etwas bewegt. Foto: mainstreamsmasher.wordpress.com

Ein Computer, der alles kann

Wie man sieht, ist bereits dieser Rauchmelder ein wahres Multitalent, das nicht nur Rauch erkennen, sondern auch das Umfeld überwachen und den eigenen Status «nach draussen» melden kann. **An Bord der meisten «Rauchmelder» befindet sich eben nicht nur eine Raucherkennungstechnik, sondern auch ein Chip, also ein Computer, der potenziell (!) alles kann, was andere Computer auch können – zum Beispiel, wenn sie in Handys installiert sind. «Wenn so ein Chip alles kann, WER definiert eigentlich, was dieser Chip WIRKLICH tut? Gibt es da eine Kontrollinstanz? Gibt es da jemanden, der reinschaut und kontrolliert, ob diese ‚eierlegende Wollmilchsau' auch wirklich NUR DAS tut, was sie soll beziehungsweise was ich so geistig als Käufer wegen der Verpackung usw. damit assoziiert habe, dass sie tun sollte? Antwort: NEIN!»**, meinte ein Insider und Elektronikexperte beim Hintergrund-Nachrichtenportal IKNews. «Eine neutrale Instanz gibt es nicht. Auch ein TÜV etc. wird [nur] die Funktion, die angemeldet wurde, prüfen, mehr nicht. Die Hersteller wehren sich mit Händen und Füssen gegen die Offenlegung.»

Vielmehr findet nun jeder interessierte Schnüffler, egal ob das nun die Staatsmacht oder elektronikbegabte Hacker sind, in Ihrer Wohnung bereits eine grosszügig gestaltete Technikplattform vor, die man entsprechend manipulieren oder austauschen kann. Die erneute Verplombung dürfte insbesondere für staatliche Schnüffler kein Problem

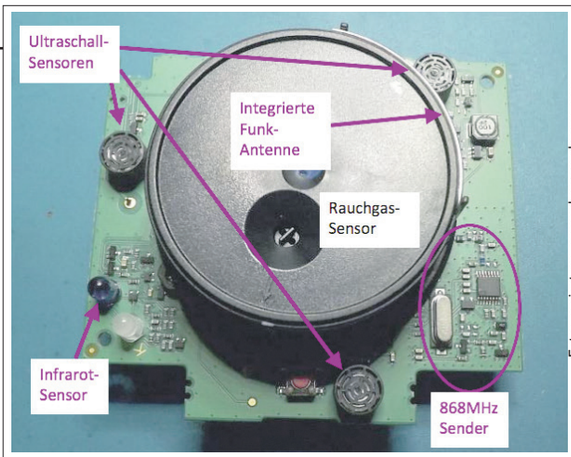
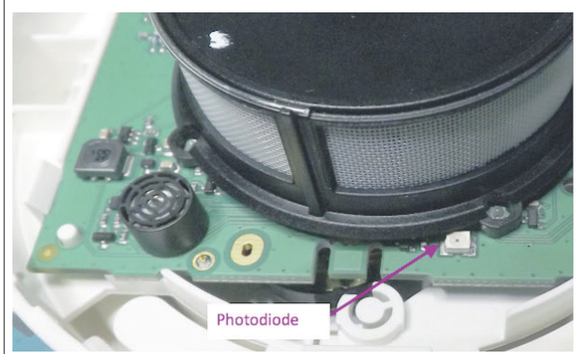


Foto: mainstrea msmasher.wordpress.com

Oberseite der Platine des Funk-Rauchwarnmelders 2 von Techem



Photodiode zur Erkennung, ob das Gehäuse geöffnet ist.

An Bord der meisten «Rauchmelder» befindet ein Computer-Chip, der potenziell (!) alles kann, was andere Computer auch können.

sein. Oder wie wäre es mit einem technikbegabten Vormieter: «Könnte es sein, dass der Installateur oder der Vormieter den Rauchmelder so manipuliert hat, dass dieser neben den normalen Rauchmelderdaten auch heikle Daten funkt, zum Beispiel wann der augenblickliche Mieter gerade nicht zu Hause ist oder ob sich im Schlafzimmer etwas bewegt? Oder kann sich ein kriminell orientierter Hacker sogar Zugang zum Mikrocontroller im Rauchmelder verschaffen, die momentan einprogrammierte Programmierung (Firmware) per Update-Funktion austauschen und damit die für die ‚Umfeldüberwachung' gedachten Mikrofone so umfunktionieren, dass zum Beispiel der Funkrauchwarnmelder 2 von Techem zur unauffälligen Abhörwanze wird?», fragt der Messingenieur Laquai.

Alle Jahre wieder kommt der ista-Mann

Wahrscheinlich können die meisten heutigen Geräte tatsächlich nur Rauch erkennen, aber gilt das auch für die Zukunft? Der Ablese-Multi ista zum Beispiel ist ein absoluter Daten-Freak und weiss eine Menge über Sie. Denn per Funk saugt er nicht nur Rauchmelderdaten ab, sondern auch «alle Daten der Heizkostenverteiler, Wärmezähler und Wasserzähler» (2). Nach Angaben des IT-Experten, der selbst in

der Branche tätig war, komme ista «jedes Jahr, reisst alle Gerätesensorik der alten Bauart ab und sammelt sie ein, also [in Bezug auf] Wasser, Heizkörper etc., und baut die neue Generation von Geräten (also die, die noch mehr können) einfach ein». So werde es auch mit den neuen Rauchmeldern sein. Die alten würden angeblich «regelmässig (normal: jährlich) gegen welche der neueren Generationen GETAUSCHT. Es wurden NIE BATTERIEN GETAUSCHT, wir haben immer eine neue Generation verbaut bekommen, jedes Jahr. Im Tausch sind die absolut fix.» Und dabei wollen wir ista und Co. gar nichts Kriminelles oder Rechtswidriges unterstellen. Bestimmt werden heute wirklich «nur» rauchbezogene Daten und Statusmeldungen des Rauchmelders übermittelt.

Aber wer sagt uns, dass die Gesetze in ein paar Jahren nicht noch eine viel weitergehende Überwachung der Wohnungen erlauben? Oder dass viele der Betroffenen diese Überwachung sogar dulden wollen – etwa wie beim Handy? Die Technik ist ja bereits vorhanden, und gewöhnt haben sich die Leute auch schon daran: Die potenziellen Wanzen an der Zimmerdecke sehen sie bald gar nicht mehr.

«My home is my castle» war gestern

Und von der Zimmerdecke aus geht es ja weiter: Bei dem ista-Funksystem mit dem schönen Namen «symphonic sensor net» werden «alle Daten von Heizkostenverteilern, Wärme- und Wasserzählern, Gas- und Stromzählern sowie von Rauchwarnmeldern per Funk übertragen.» Es gibt also Funkstrecken in unserer Wohnung, an die wir normalerweise gar nicht (mehr) denken und die wir längst vergessen haben. Prinzipiell ist der drahtlose Echtzeitzugang in unsere Behausung also schon längst eröffnet, und theoretisch könnte man auch Audio- oder Videodaten übertragen (womit nicht behauptet wird, dass dies heute schon geschieht).

«My home is my castle» war jedenfalls gestern. Unsere Wohnungen sind in Wirklichkeit

Dieser Artikel stammt aus Gerhard Wisnewskis investigativem Jahrbuch «verheimlicht – vertuscht – vergessen 2018: Was 2017 nicht in der Zeitung stand», das am 21. Dezember 2017 erschienen ist.

bereits löchrig wie ein Schweizer Käse. Die «Unverletzlichkeit der Wohnung» (Artikel 13 Grundgesetz) steht nur noch auf dem Papier. **Kommen erst noch die sogenannten «intelligenten Stromzähler» (Smart Meter, siehe S. 42) hinzu, braucht man fast schon keine Überwachungskamera mehr, um unsere Aktivitäten zu beobachten, denn anhand des Stromverbrauchs zu bestimmten Tages- und Nachtzeiten lässt sich sehr genau ablesen, was in einer Wohnung passiert.**

Doch wie konnte es nur so weit kommen? Wieso haben sich so viele Haus- und Wohnungseigentümer für den Einbau derartiger «Higtech-USOs» (Unidentified Spying Objects) entschieden? Ganz einfach: Die simplen gesetzlichen Vorschriften pusteten die Ablese- und Sicherheitskonzerne zur Pseudoverpflichtung zum Einbau von Hightech-Plattformen auf. Schauen wir uns beispielsweise eine Hochglanzbroschüre vom Marktführer ista an, die nicht nur vom Wohnungs- oder Hauseigentümer gelesen wird, sondern häufig auch von Hausverwaltungen, die gleich ganze Wohnanlagen betreuen: «Rauchwarnmelderpflicht in Deutschland – jetzt aktiv werden und gesetzlichen Anforderungen nachkommen», heisst es da gleich zu Beginn in einer grossen Überschrift. Und auf der nächsten Seite ist zu lesen: «Staatliche Regelung – gesetzliche Rauchwarnmelderpflicht zum Schutz der Bürger.» Tja – da kann man freilich nichts machen: Staat, Pflicht und Schutz sind nun einmal echte Reizworte für einen deutschen Hausbesitzer, die ihn sofort strammstehen lassen [3].

Foto: Alpnachnorm (https://commons.wikimedia.org/wiki/File:K%C3%BCche_Landhaus_3D-Laminat.jpg)
https://creativecommons.org/licenses/by-sa/4.0/deed.en

Ausgerechnet in dem Raum, in dem die meisten Brände entstehen, darf der Rauchmelder nicht installiert werden: in der Küche.

Hochsicherheitstrakt an der Zimmerdecke

Fest steht, dass damit ein quasi unerschöpflicher Geld- und Datenstrom zu den Ablesekonzernen fliesst und eine Art unangreifbarer Stützpunkt in den Wohnungen errichtet wird, an den man nicht ohne Weiteres herankommt und der für Eigentümer und Bewohner nicht durchschaubar ist. Heute sind es vielleicht noch Rauchmelder – aber morgen? Denn wenn wir einmal an eine heute allgegenwärtige Wanze wie das Handy denken, dann war es diesbezüglich ja genauso: Am Anfang konnte man mit den Geräten tatsächlich nur telefonieren. Aber kaum hatte der Verbraucher diese Technikträger einmal in der Tasche, mauserten sie sich mit zwei Kameras, GPS und Mikrofonen umgehend zum praktischen «Taschencomputer», mit dem sich der Träger auf Schritt und Tritt überwachen lässt. Das heisst: Das Gerät mutierte zur Wanze. Auch hier wurde der «Missbrauch» irgendwann zum Normalfall. Glauben Sie also wirklich, dass Rauchmelder nur Rauchmelder bleiben werden? Und das, obwohl der Standort und die extrem gesicherte Anbringung bereits ideal sind und der Platz für Sensorik und Elektronik in einem Rauchmelder natürlich viel grösser ist als in einem Handy? **Oder vermuten Sie nicht auch, dass die Konzerne schon an der nächsten Profitwelle arbeiten, nämlich an multifunktionalen und vernetzten Rauchmeldern, die im Rahmen des «Smart Homes» nicht nur Kameras und Mikrofone, sondern auch Thermometer, Luftsensoren, Erschütterungsmelder und ähnlichen Schnickschnack enthalten?**

So hatte zum Beispiel die Datenkrake Google 2011 in die Firma Nest investiert, die nicht nur «intelligente» Rauchmelder, sondern auch Überwachungskameras baut. 2014 hat Google Nest für 3,2 Milliarden Dollar übernommen. «Als Rauchmelder ist der Nest Protect von Google mit Sicherheit ein Premiumgerät», heisst es auf einer Werbeseite. «Er misst Temperatur, Kohlenmonoxid, Bewegung, Helligkeit, Ultraschall und Rauch und verknüpft all diese Informationen zu einem Gesamtlagebild». [4]

Quellen:

1. «ista: Rauchwarnmelderservice - Funktionsprüfung aus der Ferne», ohne Datum
2. ista: «Das Funksystem - Verbrauchsdaten einfach, sicher und komfortabel abrechnen», ohne Datum
3. ista: «Rauchwarnmelderservice - Funktionsprüfung aus der Ferne. Mit ista noch einfacher die Rauchwarnmelderpflicht erfüllen», ohne Datum
4. «Schlauer Schutz vor Feuer. Nest Protect Rauchmelder von Google», homeandsmart.de, 20.02.2016

Überwachung

Smart Home, Die

Über das sogenannte «Internet der Dinge» (Internet of Things, IoT) sollen in Zukunft alle Gegenstände mit Chips, Sensoren, Datenspeichern oder Softwaresystemen ausgestattet werden, um sie über das Internet miteinander zu vernetzen. Theoretisch könnten auch Menschen, z.B. durch einen implantierten Chip, im IoT vernetzt werden.

Mit «Gegenstand» bzw. «Ding» im IoT ist auch das Zuhause gemeint. Geplant ist, auf der ganzen Welt sogenannte «smart homes» (sich selbst regulierende Häuser) und daraufhin «smart cities» (sich selbst regulierende Städte) zu errichten.

Für eine Vernetzung von allen Dingen und Personen reicht die heutige Technologie für mobiles Internet allerdings nicht aus, deshalb sollen bis 2020 die neuen blitzschnellen 5G-Netze in ganz Europa installiert werden.

So verlockend das IoT auf den ersten Blick auch erscheint, es führt unweigerlich zur lückenlosen Kontrolle und Steuerung aller Dinge (und Personen?) für diejenigen, die sich seiner bemächtigen. Dazu kommen weitere Gefahren: Was ist wenn z.B. Hacker sich Zugriff auf Daten verschaffen und in ein System eingreifen? Z.B. ein Auto manipulieren, das eigenständig fährt?

Foto: Maksym Kozlenko (https://commons.wikimedia.org/wiki/File:-Coca-Cola_bottles_for_Thai_market.jpg) https://creativecommons.org/licenses/by-sa/4.0/deed.en

Foto: Genuine500 (https://commons.wikimedia.org/wiki/File:Lysol-products.jpg) https://creativecommons.org/licenses/by-sa/3.0/deed.en

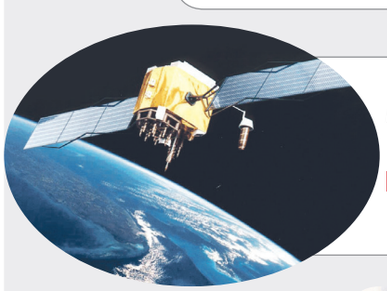
Jedes Produkt durch RFID-Chips?

siehe Seite 20

Foto: Marco Verch (https://commons.wikimedia.org/wiki/File:Smoothie-Mixer_(22590953063).jpg) https://creativecommons.org/licenses/by/2.0/deed.en

Daten von Internetunternehmen, vor allem Suchmaschinen und soziale Netzwerke

siehe Seite 7 und 11



Aufnahmen von Satelliten

siehe Seite 7

Aufnahmen und Daten von «Smart Speakern»

siehe Seite 5 und 18

Daten von digitalen Rauchmeldern?

siehe Seite 47

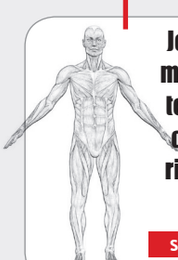
Mikrochip, GPS, Kamera und Mikrofon im Smartphone

siehe Seite 6

Foto: LG▫▫(https://commons.wikimedia.org/wiki/File:World%E2%80%99s_first_dual-core_smartphone_comes_to_europe.jpg) https://creativecommons.org/licenses/by/2.0/deed.en

Daten des Smart Homes?

siehe Seite 51 und 54



Jeder Mensch mit implantiertem RFID-Chip oder biometrischer Erkennung?

siehe Seite 25

Smart City und das Internet der Dinge –

Kontrolle über alles und jeden

Daten von digitalen Strom- und Heizungszählern

siehe Seite 42

Position und Daten digitalisierter (und bald selbstfahrender?) Autos

siehe Seite 32

IOTA

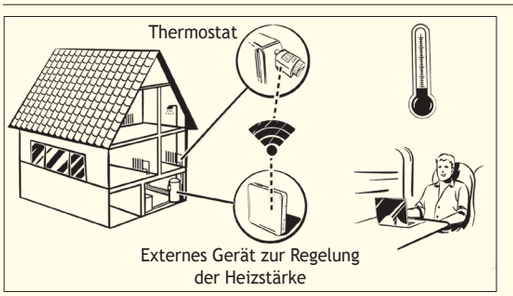
Jede Zahlung mit digitaler (Krypto-?)Währung

siehe Seite 28, 53 und 61

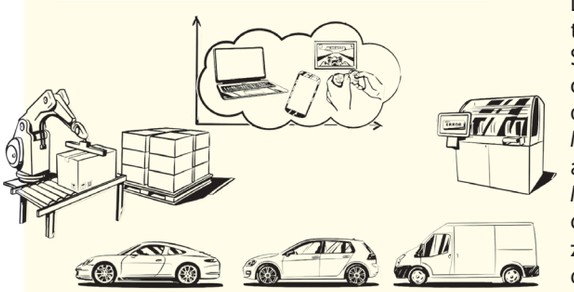
Was ist das Internet der Dinge (IoT)?

Fotos: youtube, explainity

Das Internet der Dinge (Internet of Things, kurz: IoT) ist ein Konzept aus dem IT-Bereich und bedeutet, dass Alltagsgegenstände über das Internet miteinander vernetzt sind. Sie sind mit kleinen Chips, Sensoren, Datenspeichern oder einem Softwaresystem ausgestattet. Diese ermöglichen einen Datenaustausch mit einem oder mehreren anderen Objekten. Deshalb werden sie als «smart», also intelligent, bezeichnet.

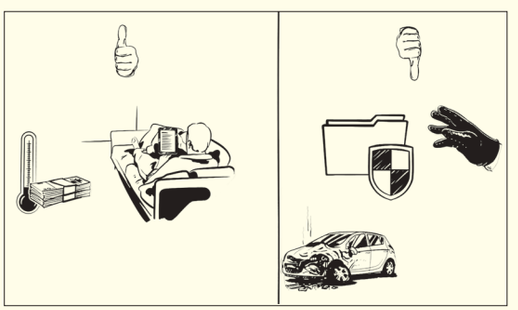


Ein Beispiel: In einem Haus befindet sich ein Thermostat mit einem Sensor. Ausserdem wurde an seinem Heizkessel ein externes Gerät mit einem Softwaresystem installiert. Beide Dinge sind mit dem Internet verbunden und heben und senken automatisch die Temperatur nach vordefinierten Werten, ohne dass der Hausbewohner vor Ort sein muss.



Den Anfang dieser Entwicklung machten Geräte wie der Laptop, das Smartphone oder die Spielekonsole. «Dinge» können aber alle möglichen Objekte sein wie Produkte, Pakete, Autos oder Industriemaschinen – theoretisch sogar Menschen. Pakete können in Logistikzentren automatisch von Robotern sortiert, Fehler in Maschinen schnell erkannt und gemeldet werden oder Autos ohne Menschen fahren. Die Anzahl der Dinge, die mit dem Internet verbunden sind, wird immer weiter ansteigen.

Befürworter sehen sehr viele Vorteile in der Automatisierung durch das IoT: Z.B. Senkung der Energiekosten oder Entlastung im Alltag.



Kritiker bemängeln allerdings die Einschränkung unserer Privatsphäre und die potenzielle Dauerüberwachung durch das IoT. Dazu kommt die Datensicherheit: Was ist, wenn Unbefugte sich Zugriff auf Daten verschaffen und in ein System eingreifen? Z.B. ein Auto manipulieren, das eigenständig fährt?

Durch das IoT sollen bald flächendeckend sogenannte «smart homes» und daraufhin «smart cities» entstehen. Ganze Städte, in denen alles miteinander vernetzt ist.

Die lückenlose Steuerung aller Dinge

Auch bei grossen Konzernen und in der Politik spielt das IoT eine immer grösser werdende Rolle. Die Idee ist es, Geräte und Gegenstände mit Sensoren und Funkchips auszurüsten, die dann ihre Informationen dem IoT zusenden. Schon heute ist diese Technologie in verschiedenen Bereichen des täglichen Lebens anzutreffen. So melden moderne Autos die Fälligkeit der Inspektion oder einen Defekt direkt an die Vertragswerkstatt; PC-Drucker senden selbstständig ihren Bedarf an Druckerpatronen zum Versandhändler. Diese Praxis soll auf alle Geräte des Alltags angewandt werden, wie z.B. Kühl- und Arzneischränke, die ihre Bestände ebenso dem IoT melden, dazu Angaben über Frischestand oder Verfallsdatum, sodass alles fein im Überblick ist. So verlockend das IoT auf den ersten Blick auch erscheint, es führt unweigerlich zur lückenlosen Kontrolle und Steuerung aller Dinge. Was ist wenn die Funkchips auch noch in Menschen implantiert werden? Wird es dann für die Herrschenden nicht allzu einfach, ihre «Schäfchen» zu bevormunden? Noch lässt sich diese Entwicklung durch Aufzeigen der Konsequenzen stoppen.

Quelle: Stimme und Gegenstimme 14/17

Mit 5G zum Internet der Dinge

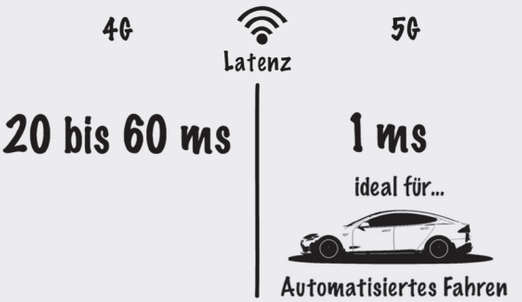
Heute greifen die Mobilfunkanbieter noch auf Netze der sogenannten dritten und vierten Generation zu (3G und 4G). Für eine Vernetzung von allen Produkten und Personen reicht die heutige Technologie für mobiles Internet allerdings nicht aus. Sie ist zu langsam und ihre Datenkapazität zu gering.

Download eines HD-Films in Sekunden, nicht Minuten

Der Schweizer Blick schreibt online über die neue 5G-Technologie, die bis 2020 flächendeckend in ganz Europa verfügbar sein soll: «Während heute mit 4G im Normalbetrieb bis zu 100 Megabit pro Sekunde erreicht werden, wird man mit 5G eine Downloadgeschwindigkeit von 10 000 Megabit erreichen, also 10 Gigabit oder 1,25 Gigabyte pro Sekunde. Das Herunterladen eines Spielfilms in 4K, das heute ein paar Minuten dauert, geht dann nur noch ein paar Sekunden. Damit hat 5G auch das Potenzial, den Internetanschluss über Kabel oder Telefonleitung teilweise zu ersetzen.»

1G	2G	3G	4G	5G
1981	1992	2001	2010	2020
2 Kbit/s	64 Kbit/s	2 Mbit/s	600 Mbit/s	15 Gbit/s

Fotos: youtube, Techstage



Schnellere Reaktion

Vielleicht noch wichtiger als das höhere Datenvolumen ist die Beschleunigung der Übertragung der Daten von A nach B (Latenz). Mit der derzeitigen 4G-Infrastruktur kämen die Informationen viel zu langsam an, vor allem im Bereich automatisierte Fahrzeugtechnologie. Mit einer Latenz von unter einer Millisekunde ist das 5G-Netz 20- bis 60mal schneller als 4G.

Der Blick bezeichnet 5G als «vor allem wichtig, da Experten davon ausgehen, dass in den nächsten Jahren weltweit Milliarden von Geräten und Diensten ans Mobilfunknetz angeschlossen werden. Es entsteht das sogenannte Internet der Dinge. So brauchen beispielsweise selbstfahrende Autos, Telemedizin oder auch intelligent gesteuerte Anlagen und Gebäude Anschluss ans Datennetz. Ländliche Gebiete können zudem einfacher und günstiger mit schnellem Internet erschlossen werden.»

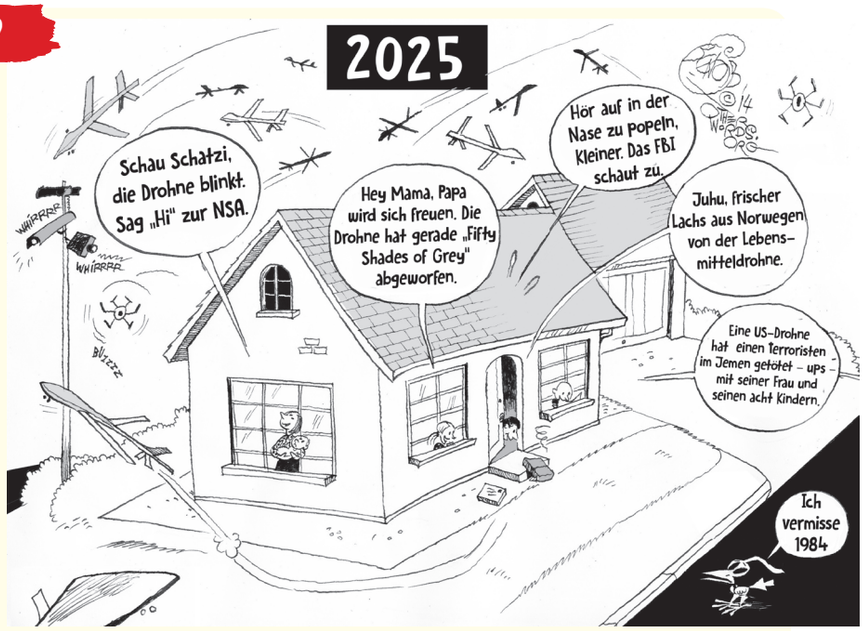
Quelle: blick.ch, Das müssen Sie über 5G wissen, 01.03.2018

Das 5G-Hightech-Gefängnis?

So akkurat kritisierte ein amerikanischer Radiomoderator das neue 5G-Netz: «5G ist eine offensichtliche Realität, die niemand sehen will. Es wird wie etwas gefördert, das sehr gut ist. Es geht um das Internet der Dinge. Was aber ist das genau? Es bedeutet, dass alles mit allem kommuniziert: Eine Breitband-Erfahrung überall und jederzeit, intelligente Fahrzeuge, Transportmittel und Infrastruktur. Das Internet der Dinge ist viel besorgniserregender als man vielleicht auf den ersten Blick denkt, denn es geht nicht nur um den intelligenten Kühlschrank, Toaster, Fernseher und das Smartphone, es geht auch um den Computer, das Mikrofon und die Kamera des Computers, sowie um das Überwachungssystem, das wir alle in unseren Heimen installieren, wenn wir die neuen Computersysteme einrichten.

Dieses System führt zu einer vollständigen digitalen Kontrolle jeder Person und einer Verschmelzung des Menschen mit künstlicher Intelligenz. Es ist praktisch die Installation eines Weltraumzauns um die ganze Erde, der aktiviert und mit dem 5G-Netz verbunden wird. Es geht darum, alles zusammenzuschliessen, die Satelliten und das 5G-Netz.

Das 5G-Netz wird eingeführt und die ganze Maschinen-Gesellschaft geht online. Wenn die Leute nicht aufpassen, weiterhin ihre Kreditkarten und Smartphones verwenden, werden sie in 5 bis 10 Jahren, wenn das gesamte Bargeld digitalisiert ist und all ihre Bewegungen und Gedanken kontrolliert und alles überwacht wird, aufblicken und sagen: ‚Moment mal! Wie bin ich in diesem Hightech-Gefängnis gelandet?' - Aber was kann man dann noch tun?»



Quelle: youtube.com, 5G Das Internet der Dinge! Jahr 2020: Vollständige technologische Versklavung!?, 10.09.2017

Ehemaliger Chef der US-Rundfunkbehörde:

Wenn etwas angeschlossen werden kann, wird es angeschlossen

Tom Wheeler war der Präsident der «Federal Communications Commission», also der US-Behörde, die die Kommunikationswege Rundfunk, Satellit und Kabel verwaltet. Kaum eine Person sollte besser wissen, was auf uns zukommt. Er beschrieb – damals noch im Amt – die Zukunft bei einer Pressekonferenz folgendermassen:

«Hunderte Milliarden von Mikrochips, die mit Produkten verbunden sind, von Pillenflaschen bis zu Rasensprengern. [...] Wir müssen die Vorstellung ablegen, dass die 5G-Zukunft allein für städtische Gebiete sein wird. Die 5G Revolution wird alle Winkel unseres Landes betreffen. [...] Amerikas lokale Regierungen werden eine wichtige Rolle bei der Umsetzung dieser nationalen Priorität spielen. Wenn etwas angeschlossen werden kann, wird es angeschlossen.»

IOTA

Wird IOTA die digitale Währung der Zukunft?

Eine der zehn wertvollsten Kryptowährungen auf dem Markt bezieht sich schon in ihrem Namen auf das Internet der Dinge: IOTA (Akronym aus Internet of Things und Tangle, abgeleitet von dem kleinsten Buchstaben im griechischen Alphabet Iota) ist ein Projekt von grossen Konzernen wie Volkswagen, der Deutschen Telekom, Samsung und vielen mehr. Im Gegensatz zu Bitcoin, dessen Ursprung bis heute im Dunkeln liegt, ist klar ersichtlich, dass IOTA ein Projekt «von oben» darstellt. Die digitale Währung wird extra dazu entwickelt, um Transaktionen im IoT möglichst schnell auszuführen. Könnte sich IOTA bald gegen Bitcoin und andere Kryptowährungen durchsetzen und uns als ideale neue Weltwährung für das IoT angeboten werden?

Will die Politik durch Digitalisierung wirklich unser Leben erleichtern?

Leser der ExpressZeitung wissen: Die heutige Politik schafft wesentlich mehr Probleme, als sie löst und erschwert das Leben der Bürger in fast allen Bereichen. Deshalb darf auch an den offiziellen Zielen der Digitalisierung (Erleichterung des Lebens, Steigerung der Produktivität usw.) gezweifelt werden, mit denen uns die allumfassende elektronische Vernetzung von Industrie und Mitgliedern aller Parteien schmackhaft gemacht wird.

Als Leser der ExpressZeitung mag man sich wundern: Von Angela Merkel über Sigmar Gabriel bis Christian Lindner, sie alle sprechen von der Digitalisierung in den höchsten Tönen. «Logisch» mag man sich im ersten Moment denken, «denn die Vorteile liegen auf der Hand: Automatisierung, Erleichterung des Alltags, steigender Komfort, höhere Produktivität und damit eine gesicherte Konkurrenzfähigkeit des Wirtschaftsstandorts Deutschland bzw. Europa.»

Foto: Armin Kübelbeck, CC-BY-SA, Wikimedia Commons

Da könnte man sich glatt entspannt zurücklehnen und mit Vorfreude dem digitalen Schlaraffenland entgegenfiebern, das auf uns zukommt – wenn man kein Leser der ExpressZeitung wäre. Denn die verlockende Utopie einer problemfreien Wohlstandsgesellschaft, in der die Technik jede Anstrengung aus dem Weg räumt, steht im starken Kontrast zu der gelinde gesagt steinzeitlichen Realpolitik, die die Bürger des Westens in letzter Zeit ertragen mussten. So sprechen Angela Merkel und die Bundesregierung in warmherzigem Ton davon, das automatisierte Fahren würde Unfälle reduzieren und die Sicherheit auf deutschen Strassen erhöhen. Doch wenn Angela Merkel wirklich die Sicherheit und der Komfort der deutschen Bevölkerung am Herzen liegt, warum brach sie im Sommer 2015 das Grundgesetz und liess hunderttausende junger Männer aus einer fremden, deutlich gewaltbereiteren Kultur unkontrolliert nach Deutschland einreisen? Heute treten die verhängnisvollen Folgen von Merkels Rechtsbruch offen zutage: Die neuen Einwanderer dominieren die deutschen Kriminalstatistiken mit Gewaltverbrechensraten in schwindelerregender Höhe.

Foto: © A.Savin, Wikimedia Commons

Strassen aus der DDR

Ähnliches gilt für den desolaten Zustand des Strassenverkehrs: Lange Staus, enge Baustellen, Schlaglöcher, Sanierungsbedarf soweit das Auge reicht. Bevor man den Deutschen wie Angela Merkel das selbstfahrende Auto ankündigt (ohne sie überhaupt danach gefragt zu haben), sollte man sie nicht erst einmal von der nahezu täglichen Tortur des Im-Stau-Stehens befreien?

Foto: twitter

Die Liste der Dinge, die die Politik unternehmen könnte, um den Normalbürgern ihr Leben zu erleichtern, kann man lange fortsetzen: Steuererleichterungen, eine stabile Währung, das Ende der massiven Einschränkung unserer Freiheit mithilfe globaler Klimagesetze ohne wissenschaftliche Grundlage, Reformierung des Gesundheitssystems zur Verbesserung des Gesundheitszustands von Patienten, bis hin zu einer Stärkung der Institution Familie, dem wichtigsten Stützpfeiler jeder gesunden Gesellschaft. All diese Bürden will die Politik nicht von unseren Schultern nehmen, doch durch die Digitalisierung will sie den überarbeiteten und von der Bürokratie erdrückten Steuerzahler endlich von der unendlichen Last des Licht-Einschaltens und Heizung-Hochdrehens befreien? Diese vermeintlich guten Absichten der Politik wirken, wie schon so oft, fundamental widersprüchlich.

Deshalb liegt auch im Fall der Digitalisierung der Verdacht nahe, dass es Merkel & Co. mal wieder überhaupt nicht um das Wohl ihrer Bevölkerung geht. So wie es auch bei der sogenannten «Flüchtlingskrise» nicht um selbstlose Hilfe für unschuldige Kriegsopfer, sondern um eine lang geplante Migrationsagenda; beim vermeintlich «menschgemachten Klimawandel» nicht um Umweltschutz, sondern um die Kontrolle menschlicher Handlungen; beim Feminismus nicht um Frauenrechte, sondern um die Auflösung der Familie geht, so scheint es bei der Digitalisierung in Wahrheit auch nicht um mehr Komfort, Sicherheit und Entlastung für den Otto-Normalbürger zu gehen, sondern um die Schaffung eines gläsernen Bürgers durch mehr Überwachung und Kontrolle. ***(tk)***

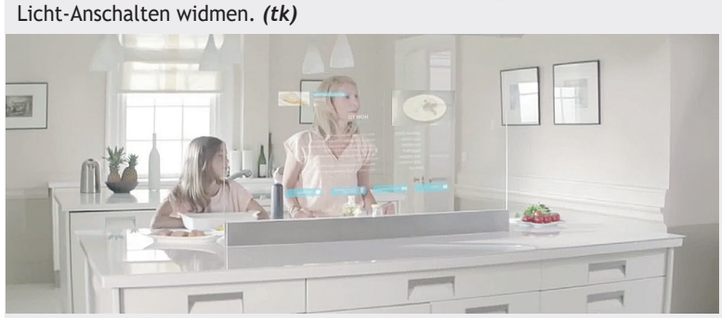
Smart home - Braucht man das?

Auch bei der Vermarktung der neuen «smart homes» strahlt die Zukunft in den hellsten Farben: Traumfamilien kochen, essen und spielen in ihren voluminösen Eigenheimen, die ihnen mit allerlei High-Tech das Leben noch angenehmer machen. Doch was haben ein grosses Haus und eine Familie überhaupt noch mit der Realität des Durchschnittsbürgers zu tun? Viele Deutsche haben mittlerweile aus Geldnot Angst davor, eine Familie zu gründen. Oft reicht das Geld gerade noch für die Miete ihrer Zwei-Zimmer-Wohnung. Leider wirkt die Zukunftsvision aus den Werbespots für die Mehrheit der Deutschen unerreichbar. Es stellt sich deshalb die Frage: Für wen werden diese smart homes entwickelt? Für den Normalbürger sicher nicht! Etwa für die Vorstände der Grosskonzerne, die sie bauen? Für Minister wie Sigmar Gabriel, die nach ihrem Engagement für das Verbot manuell steuerbarer Autos, vielleicht einen profitablen Vorstandsposten bei Daimler-Benz bekommen?

Diejenigen aus dem oberen Mittelstand, die sich mit Ach und Krach so ein smart home leisten könnten, stünden dann vor der Entscheidung, ob ihnen das kleine Plus an Komfort im Vergleich zu einem normalen Haus das Geld wirklich wert ist. Was kostet die Instandhaltung der Software? Was kostet der Service, wenn ein Programm abstürzt? Muss das Haus regelmässig geupdatet oder die Hardware alle zehn Jahre getauscht werden? Und dieser ganze Aufwand nur, damit sich die Rollläden von selbst öffnen, sich die Heizung und das Licht selbst regulieren oder die Tür sich automatisch verriegelt? Um diese vollkommen trivialen und nebensächlichen Probleme, deren Existenz wir vor der Digitalisierung nicht einmal bemerkten, zu lösen, sollen wir unser Haus tausenden gleichzeitig ablaufenden Rechenprozessen unterwerfen, die sowohl stör- als auch hackeranfällig sind und gleichzeitig noch unsere Dauerüberwachung ermöglichen?

Das smart home soll Probleme lösen, die wir nie gehabt haben. Oder war es für Sie jemals ein Problem, die Heizung hochzudrehen, wenn Sie fröstelten oder das Fenster aufzumachen, wenn die Luft im Zimmer stickig war? War es jemals ein Problem, das Haus eines Freundes anzusteuern, den man besuchen wollte? War es jemals ein Problem, Milch zu kaufen? Die Probleme, die smart homes lösen, sind triviale Probleme. Das heisst: Für das Leben ist es total egal, ob sie «gelöst» werden oder nicht. Anders verhält es sich z.B. mit nicht trivialen Problemen. Das sind z.B. Ungerechtigkeit, Unterdrückung, Gewalt, die Ausnutzung von Macht – Dinge, die die komplette Geschichte der Menschheit durchziehen, ohne je gelöst worden zu sein – bis zum heutigen Tag.

Wir wollen nicht fortschrittsfeindlich klingen: Doch es gibt zu viele andere echte Probleme in dieser Welt, die es zu lösen gilt, bevor wir uns dem Licht-Anschalten widmen. ***(tk)***



Welche reale Familie entspricht heute noch den wohlhabenden Traumfamilien aus den Smart-Home-Werbevideos? Nur ein Bruchteil der Bevölkerung wird sich diese digitalen Häuser leisten können, deren Mehrheit voraussichtlich aufgrund des mangelhaften Kosten-Nutzen-Verhältnisses dennoch darauf verzichten wird. Als Kunden bleiben dann fast nur noch die ultrareichen Profiteure des Systems.

Foto: Shutterstock/ Sergey Nivens

Die

Sicherheit war im Laufe der Geschichte immer ein beliebtes Argument der Herrschenden, um die Bevölkerung für ihre Massnahmen zu gewinnen. Auch bei der Digitalisierung wird oft von erhöhter Sicherheit gesprochen, die eine vernetzte Welt bietet.

Unlängst ging durch die Medien, dass zwei Hacker sich in die Bedienung eines fahrenden Autos eingeschaltet hatten und den (vorher eingeweihten) Fahrer damit verblüfften, dass sie das Radio oder die Scheibenwischer nach Belieben ein- und ausschalten und den Motor lahmlegen konnten. Der Fahrer sass entmächtigt in seiner Kiste. Sein Auto fuhr ihn, nicht er das Auto. Was ist, wenn Sie in Ihr Auto steigen und beim gelangweilten Blick aus dem Fenster plötzlich bemerken, dass die Türen verriegelt wurden und auch die elektrischen Fenster nicht mehr reagieren. Jemand hat die Kontrolle über Ihr Auto übernommen und fährt Sie in ein Gewerbegebiet, ganz weit draussen, in eine Lagerhalle. So könnten Entführungen im digitalen Zeitalter aussehen.

Die digitale Welt hat regelmässig mit Angriffen von aussen zu kämpfen: All die schönen nietennagelneuen X-Boxen, 2014 in den USA unter dem Weihnachtsbaum gelegen hatten, liefen infolge eines Hacker-Angriffs nicht. Doch selbst wenn die moderne Elektronik nicht zu hacken wäre: Drei Tage ohne Strom reichen, um die digitale Welt vollständig lahm zu legen. Genauso wie Ihnen drei Tage ohne Wasser oder sieben ohne Nah-

Das Ende

Selbst eine totalitäre Gesellschaft, wie wir sie von früher kennen, z.B. die DDR, hielt Nischen bereit, die vom Regime nicht eingesehen werden konnten. Private Räume, die man zur Konspiration, zum Unterleben der Gesellschaft nutzen konnte. Niemand hat in tyrannischen Systemen als einzelner überlebt; wenn jemand gerettet wurde oder sich retten konnte, dann mit Hilfe sozialer Beziehungen. Das bedeutet: Räume des Privaten, zu denen von aussen niemand Zugang hat, sind essentiell dafür da, dass sich jemand noch unter totalitären Bedingungen vor Verfolgung schützen kann.

Heute gibt es keine Nischen mehr. Alle sozialen Felder, alle räumlichen Nischen sind taghell ausgeleuchtet. Was heisst: Es wird nicht nur niemand gerettet. Es gibt auch keinen Widerstand. Heute haben wir es mit einer fatalen Symbiose zweier Überwachungsmaschinerien zu tun, nämlich einer staatlichen und einer privaten. Womit wir de facto konfrontiert sind, ist eine staatlich-privatwirtschaftliche Formation zur Erzeugung von informationeller Macht über Menschen. Diese Formation macht die totale Überwachung von Menschen so perfekt umsetzbar wie noch nie zuvor in der Geschichte der Menschheit. Die dunkle Vision eines sehr klugen Vorreiters der Rasterfahndung und Datenauswertung, des früheren Chefs des Bundeskriminalamtes Horst Herold, 1980 formuliert, ist längst Wirklichkeit geworden:

«Die Grenzenlosigkeit der Informationsverarbeitung» schrieb er in einem Aufsatz über «Polizeiliche Datenverarbeitung und Menschenrechte», «wird es gestatten, das Individuum auf seinem gesamten Lebensweg zu begleiten, von ihm laufend Momentaufnahmen, Ganzbilder und Profile seiner Persönlichkeit zu liefern, Lebensformen und Lebensäusserungen zu registrieren, zu beobachten, zu überwachen und die so gewonnenen Daten ohne die Gnade des Vergessens ständig präsent zu halten.» 1980 gab es noch kein Internet. Kein Handy. Kein Smartphone. Keine E-Mail. Keine SMS. Kein Twitter. Kein Whatsapp. Überhaupt keine Apps. Keine Kameras in Telefonen, Autos, auf Fahrradhelmen. Keine Drohnen.

Verletzlichkeit der digitalen Welt

rung reichen, um zu sterben, auch wenn Sie ein 1A-funktionierendes Smartphone besitzen.

Was passiert bei einem Stromausfall?

Marc Elsberg hat in seinem Roman Blackout gezeigt, was alles nicht mehr funktioniert, wenn grossflächig der Strom ausfällt. Das sind Dinge, auf die man so schnell nicht kommt: Fahrstühle, Rolltreppen, Licht, Warmwasser, Kühlschrank – das ist klar. Aber wer denkt darüber nach, dass man nicht mehr tanken kann, weil die Zapfsäulen Energie benötigen, genauso wie Verkehrsampeln, Strassenbeleuchtungen, Bankautomaten, Strassenbahnen, Züge – also die komplette Infrastruktur unseres ganz normalen Alltagslebens? Wer kommt dann wie zur Arbeit, zur Schule, zum Dienst? Das alles ist aber noch harmlos: Weiter geht es mit dem Ausfall von Kühlanlagen in Supermärkten und Atomkraftwerken, den Sicherungseinrichtungen in Gefängnissen und wenn es lange genug dauert den Notstromaggregaten in Krankenhäusern und Sicherheitszentralen usw.

Die digitale Welt ist einem solchen Fall in kurzer Zeit schlicht und einfach inexistent, und die analoge steckt in allergrössten Schwierigkeiten, weil die Vernetzung das System ja insgesamt so verletzlich gemacht hat, dass viele Teilsysteme eben nicht mehr autonom funktionieren. Denn die ganze Wundermaschine der Digitalisierung hat ein systemisches Problem: Sie ist nicht autark. Sie funktioniert nicht autonom, sondern nur in Abhängigkeit – deshalb ist sie nach aussen offen und daher grundsätzlich angreifbar und prinzipiell verletzlich. Absoluten Schutz, und das demonstriert nicht nur das gehackte Auto, gibt es nicht. Was aber noch gravierender ist: Die Maschine hängt, das zeigt Blackout eindrucksvoll, von externer Energiezufuhr ab, weshalb all die Programme, all die Serverfarmen, all die Überwachungszentralen nicht mehr

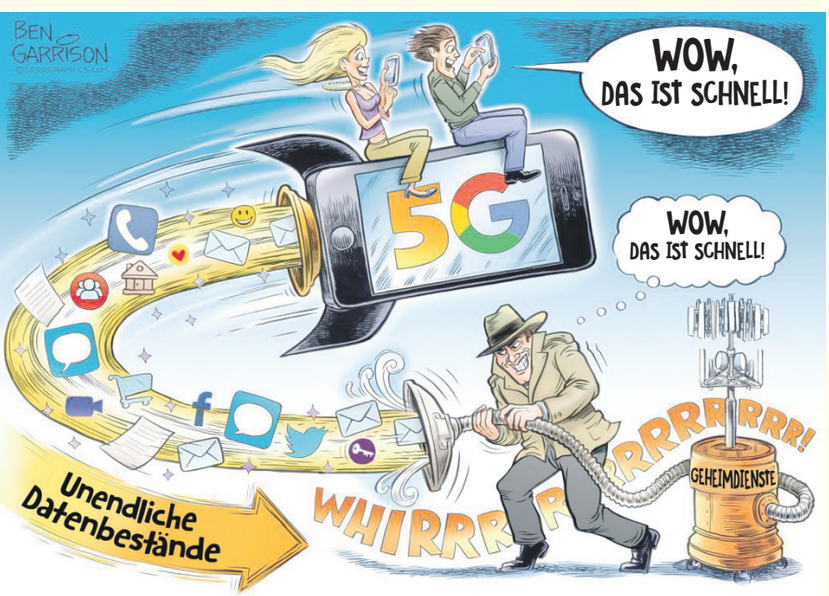
Foto: Shutterstock/Chesky

Bedeuten selbstfahrende Autos wirklich mehr Sicherheit? Hacker können heutzutage nachweislich die Kontrolle über jedes Auto gewinnen. Inzwischen werden sogar manche Unfälle moderner Autos von kritischen Stimmen hinterfragt und eine Untersuchung des Bordcomputers gefordert (siehe S.64). Die Abgabe der Eigenverantwortung am Steuer birgt schwere Risiken in sich, die Politik, Medien und Grosskonzerne nur selten ansprechen.

als nutzloser Plunder sind, wenn der Strom lange genug ausfällt. Und die Maschine braucht Input, sonst läuft sie nicht. Fällt nur einer dieser Faktoren aus, wird die angeblich so intelligente Maschine blitzartig, von einer Sekunde auf die andere, dumm wie ein Stein.

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.

der Privatsphäre



Das Panoptikum

Das ist das panoptische Prinzip: Wir alle sind permanent sichtbar, also kontrollierbar, sehen aber nicht die, die uns sehen. Und noch etwas: Wir alle sind sichtbar, aber nicht füreinander. Diese Machttechnologie verändert unser Selbstverhältnis: Wir verfügen über weniger Wissen über uns selbst als andere, die wir nicht einmal kennen. Daraus folgt exakt das, was der notorische Eric Schmidt, ehemals CEO von Google, in frappierender Offenheit so formuliert hat: «Wenn man nicht will, dass bestimmte Handlungen negativ in der Öffentlichkeit präsentiert werden, dann sollte man sich überlegen, diese Handlungen erst gar nicht zu vollziehen.»

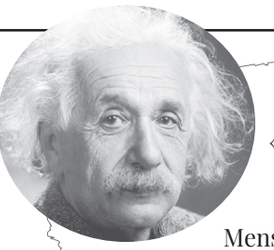
Und noch etwas liegt in der Universalisierung des panoptischen Prinzips: es ist nicht mehr nötig, sich abweichend zu verhalten, um Objekt permanenter Beobachtung zu werden. Niemand muss mehr kriminell, soziopathisch, terroristisch oder auf andere Weise gemeingefährlich sein, um unter Aufsicht gestellt zu werden. Man steht grundsätzlich unter Aufsicht, was gleichbedeutend ist mit: Unter Verdacht. Und wie in der Quantentheorie genügt eine kleinstmögliche Zustandsveränderung, damit aus dem Verbrecher oder Abweichler im Latenzzustand ein wirklicher Abweichler wird.

Foto: I, Friman

Ein Panoptikum ist der Aufbau eines Gefängnisses, bei dem der Wächter im mittleren Turm für die Gefängnisinsassen unsichtbar ist. Heute sind wir im übertragenen Sinn die Gefängnisinsassen, die von den Tech-Konzernen und Geheimdiensten im Turm beobachtet werden.

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.

Foto: shutterstock/PKpix



«Ich fürchte mich vor dem Tag, an dem die Technologie unsere Menschlichkeit übertrifft. Auf der Welt wird es nur noch eine Generation aus Idioten geben.»

Albert Einstein

Isolation durch digitale Medien

Durch das ständige Starren in digitale Medien findet immer weniger zwischenmenschliche Konversation und echte Interaktion miteinander statt. Die Isolation der Menschen voneinander war schon immer ein wichtiger Eckstein der totalitären Kontrolle: Die menschliche Lebensform ist die der wechselseitigen Beziehung, kein Mensch wird allein, ohne ein soziales Beziehungsgeflecht, erwachsen. Totalitarismus ist vor allem daran interessiert, autonome Beziehungen zu zerstören, die Menschen also voneinander isolieren. Erst in diesem Zustand kann totale Beherrschung stattfinden. Verlassenheit und Isolation bilden die perfekte Voraussetzung dafür.

Die verführerische Entlastung von der Freiheit

«Freiheit von» ist nicht das gleiche wie positive Freiheit, nämlich «Freiheit zu». Das heisst: Freiheit ist nicht einfach nur ein Gewinn für die Individuen wie für die Gesellschaft, sondern sie kostet auch etwas, bedeutet chronische Orientierungs- und Entscheidungsnotwendigkeit. Freiheit ist deshalb immer auch eine Zumutung für den Einzelnen, und es ist kein Zufall, dass Gesellschaften immer Räume angeboten haben, sich von dieser Zumutung zu entlasten: durch Rituale, Rausch, Massenereignisse, Saalschlachten, Fansein im Stadion. Man kann auch die Welt des Digitalen über weite Strecken als Verführung zur Entlastung von Freiheit betrachten – Sie müssen ja heute nicht einmal mehr entscheiden, welche Musik Sie für Ihre Joggingrunde am Morgen aussuchen, das macht Spotify für Sie. Und künftig fährt Sie Ihr Auto autonom irgendwohin, Sie brauchen nicht einmal dafür mehr Aufmerksamkeit und Selbstkontrolle, sondern können sich allen Unterhaltungs- und Informationsangeboten hingeben, selbst wenn Sie mit 200 über die Autobahn rauschen. Sie sind frei von jeder Verantwortung. Aber zu was sind Sie frei?

Die totalitäre digitale Gesellschaft zeichnet sich dadurch aus, die Menschen von der Freiheit zu entlasten, ihnen die Zumutung des eigenen Entscheidens abzunehmen.

«Wir wissen nicht […], aber wir können es ahnen, wie viele Menschen in Erkenntnis ihrer wachsenden Unfähigkeit, die Last des Lebens unter modernen Verhältnissen zu ertragen, sich willig einem System unterwerfen würden, das ihnen mit der Selbstbestimmung auch die Verantwortung für das eigene Leben abnimmt.»

So hat es Hannah Arendt formuliert, und auch Sebastian Haffner hat als grösste Attraktion der totalitären Gesellschaft die völlige Ablehnung von Verantwortung für sich selbst gesehen. Es wird deutlich: Angebote zur Abgabe von Verantwortung wirken entlastend, Freiheitsangebote belastend.

Quelle: Harald Welzer, Die smarte Diktatur – Angriff auf unsere Freiheit, 2016, Fischer Verlag GmbH.

Foto: Olaf Kosinsky/Skillshare.eu

«Die Macht der digitalen Revolution liegt darin, dass kein Mensch gezwungen wird, mitzumachen. Jeder will dabei sein und tut es aus freien Stücken.»

Sigmar Gabriel

Foto: shutterstock/Kit8.net

In der Welt der digitalen Überwachung lässt sich durch die Bündelung statistischer Daten (Metadaten) über eine Person mehr herausfinden, als ihre offiziellen Rohdaten (z.B. ein Steckbrief) verraten. So stellte sich z.B. der SPD-Bundestagsabgeordneten Sebastian Edathy, gegen den wegen des mutmasslichen Besitzes von Kinderpornographie ermittelt wurde, auf seiner Webseite mit den Hauptthemen Innere Sicherheit, Staatsbürgerrecht, Atommüll-Endlagerung und Untersuchung des «Nationalsozialistischen Untergrunds» vor (Rohdaten). Da er, wahrscheinlich ohne es zu bemerken, auf seiner Website dauernd das Wort «Kinder» benutzte (Metadaten), hätte man seine perverse Vorliebe schon früh bemerken können. Die Metadaten verrieten also mehr über ihn als seine Rohdaten.

Das Problem an Metadaten ist jedoch, dass sie lediglich einen Verdacht unterfüttern und auch einen falschen Eindruck erzeugen können. Ein Ermittlungsverfahren darf nicht allein wegen der häufigen Verwendung des Wortes «Kinder» auf der eigenen Website eingeleitet werden. Doch die Entwicklung, dass Menschen allein anhand ihrer Metadaten verdächtigt werden, schreitet immer weiter voran.

Diese Entwicklung der ständigen Beobachtung «auffälligen Verhaltens» könnte bald in einem «Sozialen Kreditsystem» nach chinesischem Modell enden, das bereits in vielen Gebieten eingeführt wurde und bis 2020 alle Bewohner Chinas erfassen soll. Wer sich systemkonform verhält, bekommt mehr Punkte, wer sich an den gerade aktuellen Vorgaben des Staates «versündigt», bekommt Punkteabzug.

Durch Smartphones, Computer, das Internet und die Digitalisierung hat ein Paradigmenwechsel in der Überwachung stattgefunden: Vom Zwang zur Freiwilligkeit. Heute muss man niemanden mehr heimlich verwanzen, um an sein Privatleben zu kommen. Inzwischen steht der moderne Mensch Schlange für seine Wanzen.

Obwohl Kryptowährungen sicher im Moment eine bessere Alternative zum Geld der Zentralbanken darstellen, wirkt es, als würden sie nach dem gleichen Prinzip funktionieren: Das Bedürfnis nach dem digitalen Angebot könnte künstlich erzeugt werden, um über das elektronische Geld noch mehr Transaktionen in den bargeldlosen Bereich hineinzuziehen. Auch hier könnte also ein Zwang in eine Nachfrage verwandelt werden, um daraufhin alle Kryptowährungen unter staatliche Kontrolle zu stellen.

von Gerhard Wisnewski

Foto: Shutterstock/Valery Brozhinsky

Überwachung:

Wer rennt, ist verdächtig
Resümée und Ausblick

Bei der Lektüre dieser Ausgabe unserer Zeitung werden Sie es schon gemerkt haben: Seit den Zeiten des Thrillers «Staatsfeind Nr. 1» und erst recht von George Orwells Roman «1984» hat beim Thema Überwachung ein Paradigmenwechsel stattgefunden: Und zwar vom Zwang zur Freiwilligkeit, von der Nötigung zum Bedürfnis und von der Heimlichkeit zur Offenheit. Eine Überwachung, vor der sich jeder zu drücken versucht, ist nun einmal nicht optimal. Viel besser sind Schnüffeleinrichtungen, um die sich die Leute reissen. Wurden in dem Roman 1984 von George Orwell die Menschen gegen ihren Willen bespitzelt, werden heute ihre Bedürfnisse ausgenutzt. Während die Hauptperson aus «Staatsfeind Nr. 1» verzweifelt vor ihren Häschern floh, laufen wir ihnen heute freudig in die weit ausgebreiteten Arme. Sprich: Heute muss man niemanden mehr heimlich verwanzen, um an sein Privatleben zu kommen. Inzwischen steht der moderne Mensch Schlange für seine Wanzen: Ob das nun Smartphones, Fitnessarmbänder oder elektronische Assistenten für zu Hause sind. Dieser gewaltige Paradigmenwechsel birgt enorme Vorteile: Wanzen werden nicht gemieden, sondern nachgefragt. Mikrophone und Kameras müssen nicht heimlich eingebaut werden, sondern werden von den Zielpersonen gekauft. Und Zielperson sind wir alle: Die flächendeckende Verwanzung der

→

Seite 57

Erdbevölkerung mit mobilen Luxuswanzen vom Typ Iphone, Samsung Galaxy oder Amazon Echo würde kein Staat und keine internationale Organisation logistisch und finanziell hinbekommen, wenn die Verbraucher das nicht selbst besorgen würden. Daten müssen den Opfern nicht mühsam aus dem Kreuz geleiert werden, sondern werden von den betroffenen Menschen höchstpersönlich eingetippt. Begeistert führen sie ihre elektronische Akte selber – jeden Tag, jede Stunde und sogar jede Minute. Programme und «Apps» müssen nicht unbedingt auf den Computer oder das Handy geschmuggelt werden, sondern werden freiwillig installiert, ohne dass jemand die ellenlangen Nutzungsbedingungen liest. Denn selbst wenn man sie lesen würde, würde man die Konsequenzen all der Bestimmungen gar nicht überblicken.

Die Macht der Metadaten

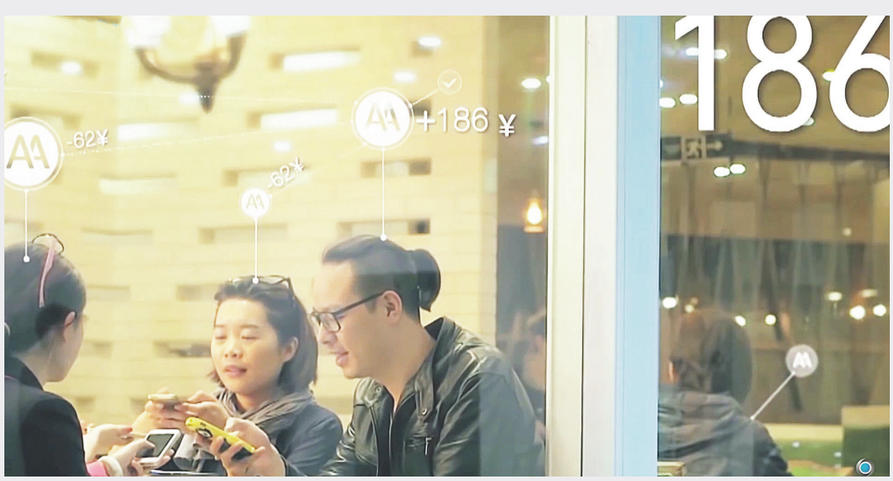
Ausserdem: Bei der Überwachung gibt es niedrigere und höhere Funktionen. Wie in dem einleitenden Artikel über die verschiedenen Schnüffeltechniken bereits angedeutet, bestehen niedrige Funktionen in einzelnen Techniken, die zu einzelnen Erkenntnissen führen. Höhere Funktionen bestehen in der Bündelung der einzelnen Quellen und in der Auswertung ihrer Ergebnisse. Man kann sagen, dass der Mensch, sobald alle seine Daten gebündelt sind, schon heute total transparent ist – und zwar transparenter als für sich selbst oder für seine Ehefrau. Das liegt daran, dass seine übergeordneten «Metadaten» mehr über ihn aussagen als seine «Rohdaten» – also beispielsweise ein geschriebener Klartext. Die statistische Verteilung benutzter Begriffe kann viel interessanter sein. Nehmen wir nur kurz das Beispiel des früheren deutschen SPD-Bundestagsabgeordneten Sebastian Edathy, gegen den spätestens ab 2013 wegen des mutmasslichen Besitzes von Kinderpornographie oder zumindest von Kindernacktbildern ermittelt wurde. Anhand eines sehr einfachen Experiments konnte ich damals die Macht der Metadaten demonstrieren.

«Innenexperte» auf Abwegen

Eigentlich war Edathy ein Innenexperte mit den Hauptthemen Innere Sicherheit, Staatsbürgerrecht, Atommüll-Endlagerung und vor allem «NSU», also «Nationalsozialistischer Untergrund». Ab Januar 2012 leitete er sogar einen Untersuchungsausschuss des Bundestages zu der Terrorgruppe. Am meisten interessierten den ledigen und kinderlosen Innenexperten jedoch nicht etwa Kriminellle und Terroristen, Atommüll und Staatsbürgerschaften, sondern Kinder. Das legte jedenfalls Edathys Website nahe, wo er eine umfangreiche Sammlung aus eigenen Pressemitteilungen und diversen Zeitungs-

China hat ca. 100 Millionen Kameras auf seinen Strassen installiert - die höchste Anzahl der Welt. Ausserdem verfügt das Land bereits über «smarte» Kameras der nächsten Generation, die Daten von Autos und Menschen registrieren und wiedergeben.

Mit diesen Kameras kann sogar die Stimmung der Gefilmten analysiert werden. Theoretisch könnte in es im chinesischen «Sozialen Kreditsystem» bald Abzüge für schlechte Laune geben oder es könnte gar zu präventiven Verhaftungen kommen, da schlechtgelaunte Menschen eher zu Kriminalität und Terror neigen könnten.



Bald könnte jede Bewegung und jeder Gesichtsausdruck in die Bewertung des chinesischen Bonitätssystems einfliessen. Dagegen erscheint die Bespitzelung durch den Nachbarn im untergegangenen Stasi-Staat DDR regelrecht harmlos.

artikeln zusammengestellt hatte, die in ihrer überwiegenden Mehrheit überhaupt nichts mit Kindern zu tun hatten. Wer aber auf diesem Internetauftritt das Wort «Kinder» in das Suchfeld eintippte, erhielt nicht weniger als 320 Treffer. Bei Edathys eigentlichem Spezialthema – der Terrorgruppe «NSU» – fand man dagegen nur 171 Treffer, also halb so viele. Bei dem Wort «Senioren» gab es nur 38 Fundstellen, bei Behinderten 37. Egal, welche soziale Gruppe man auf Edathys Website auch suchte, sie landete weit abgeschlagen hinter Kindern («Migranten» 125 Treffer, «Ausländer» 73). Auch für Kriminalität (17) schien sich der Innenpolitiker kaum zu interessieren. Man darf darauf wetten, dass ihm das nicht einmal selber aufgefallen ist (das Verfahren wegen des Besitzes von Kinderpornographie wurde übrigens gegen Zahlung von Euro 5.000 eingestellt).

Der Fall Edathy ist nur ein kleines, einfaches Beispiel dafür, wie man mit Hilfe von Metadaten Dingen auf die Spur kommen kann, die der betreffende wahrscheinlich noch nicht einmal selber bemerkt hat – zum Beispiel, dass er auf seiner Website dauernd das Wort «Kinder» benutzt. Solche Metadaten sind also alles andere als harmlos. Zum einen, weil sie auch einen falschen Eindruck erwecken können, zum anderen, weil davon trotzdem Leben und Tod abhängen können. Aufgrund von «Metadaten» starten die USA sogar tödliche Drohnenangriffe: Also nicht auf der Basis von Beweisen in irgendwelchen Dokumenten oder abgehörten Gesprächen, sondern aufgrund von Verbindungsdaten, also nicht was, sondern mit wem eine Person gesprochen hat. War der Gesprächspartner zum Beispiel ein gesuchter Terrorist, wurde auch die nächste oder übernächste Kontaktperson so eingestuft und unter Umständen von einer Drohne getötet. Und das wird nicht etwa als Mord, sondern als Kriegführung gesehen, wo man ja auch ein bestimmtes Areal beschiesst und dabei ohne Ansehen der Person alles tötet, was dort kreucht und fleucht - einfach, weil es quasi allein durch seine Nähe zu einem Ziel diesem Ziel zugerechnet wird.

Wer rennt, ist verdächtig

Diese «höheren Überwachungsfunktionen» schreiten immer weiter voran. In der deutschen Stadt Mannheim wird daran gearbeitet, menschliches Verhalten automatisch zu erkennen und zu melden. «Der Erste Bürgermeister und Sicherheitsdezernent der nordbadischen Stadt arbeitet zusammen mit Polizeipräsident Thomas Köber am Konzept ‚Mannheimer Weg 2.0'. Dieser Weg umfasst ein ‚intelligentes Kamerasystem', das quasi selbstständig Strassenkriminalität erkennen und Polizisten alarmieren soll», so Spiegel Online am 15. Februar 2018. Besonders suspekt: «hektische oder untypische Bewegungen». «Rennen und Fallen» könnten in Mannheim «bald verdächtig» sein. Wer rennt, könnte ja ein Taschendieb sein, oder wer hinfällt, ein Opfer eines Verbrechens.

Oder nehmen wir das Beispiel Israel. Dort kann man angeblich vorhersagen, «wer Terrorist wird». Und zwar noch bevor es der künftige Täter selber weiss: «Oftmals wussten die Täter am Abend zuvor selber nicht, dass sie bald einen Anschlag begehen würden», zitierte die Welt einen Militär: « ‚Wenn ich jemand ausmache, der die ganze Nacht im Internet aktiv ist, sich dort für gewisse Dinge interessiert, bestimmte extremistische Kommentare abgibt, und danach mit gewissen Leuten spricht – dann gehen in unseren automatisierten Systemen die Warnleuchten an.' Die Computer setzen erfahrene Geheimdienstler auf die potenziellen Täter an. [...] Vor einem Monat habe man eine Attentäterin auf dem Weg zu ihrer Tat entdeckt. ‚Wir schickten die Beamten zum Taxi, mit dem sie zur jüdischen Siedlung in Hebron fuhr. In ihrer Handtasche fanden sie ein grosses Messer'» [1].

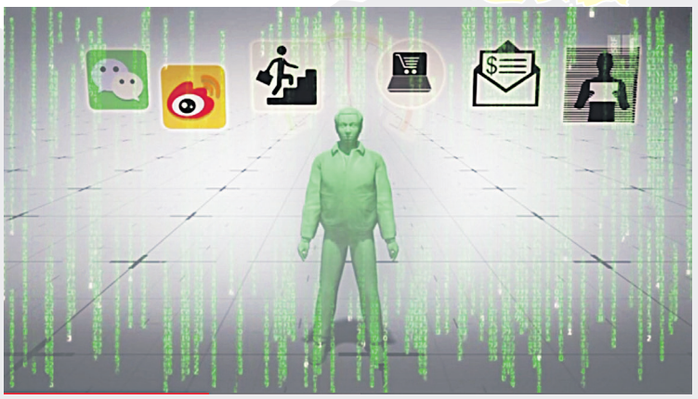
Das Weltwirtschaftsforum plant die Tyrannei

Im Januar 2018 brachte das Wetwirtschaftsforum in Davos eine regelrechte Horrorvision heraus. Titel: «Der bekannte Reisende. Die Erschliessung des Potenzials der digitalen Identität für ein sicheres und reibungsloses Reisen» [2]. Sicher und reibungslos sollen unsere Reisen natürlich nur für den Staat oder die Staaten werden. Die Idee: In einer Datenbank soll der Reisende selbst seine Daten sammeln, als da wären «Bankdaten, Hotelübernachtungen, Mietwagenbuchungen, Dokumente von Universitäten, Ämtern etc.» Sobald wir eine Grenze überschreiten wollen, sollen wir «den Behörden freiwillig einen Zugang zu diesen Daten» geben, zitierte die Website cashkurs aus dem Dokument, «damit sie sich vorab überzeugen können, dass wir harmlos sind». Was nicht nur eine Verhöhnung des Datenschutzes darstellt, sondern auch eine Verhöhnung der Bürger und der Menschenwürde: Sie selbst sollen gezwungen werden, ihre eigenen Daten zu sammeln und an die «Sicherheitsbehörden» zu übergeben. Sonst dauerts an der Grenze eben extra lange. Wer sich das Dokument des Weltwirtschaftsforums näher ansieht, ahnt wohin der Hase läuft. Und das liegt an dem kleinen Wörtchen «state» in dem Slogan des Weltwirtschaftsforums: «Committed to improving the state of the world». «State» kann nämlich sowohl «Zustand» als auch «Staat» heissen. Also bedeutet der Slogan entweder: «Der Verbesserung des Zustandes (state) der Welt verpflichtet» oder: «Der Verbesserung des Weltstaates verpflichtet».

Schon vor vielen Jahren, 1970, befürwortete der berüchtigte amerikanische Geostratege Zbigniew Brzeziński in seinem Buch Between Two Ages: America's Role in the Technotronic Era «die Kontrolle der Bevölkerung durch die herrschende politische Klasse mithilfe moderner, insbesondere elektronischer Technologien». Mindestens so lange wird die digitale Tyrannei also schon geplant. Die modernen Kommunikationstechniken sollen eingesetzt werden, «um die Gefühle zu manipulieren und das Denken zu kontrollieren», so Brzeziński. «Eine solche Gesellschaft wird von einer Elite beherrscht, die sich nicht an traditionelle Werte gebunden fühlt» [3]. Eine erstaunliche Aussage. Im Kern sind das wohl die zehn Gebote.

Foto: Kleinschmidt / MSC

Fotos: SRF



Das staatlich verordnete «Soziale Kreditsystem» in China erfasst alle Online-Aktivitäten vom Chat bis zum Shopping, aber auch Finanz- und Strafregisterdaten.

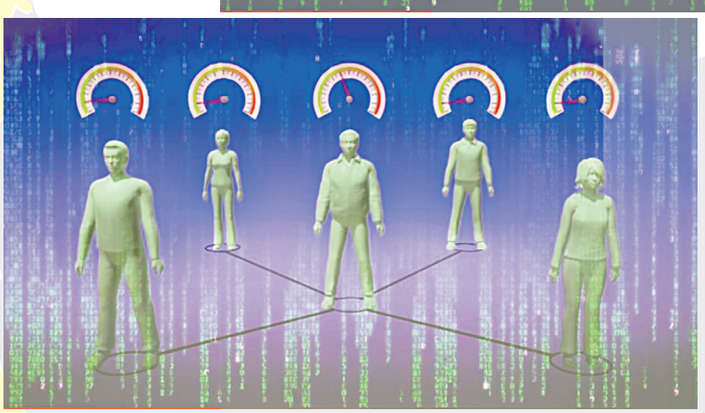
Es errechnet daraus einen «Sozialen Kreditwert». Statuspunkte gibt es für regierungstreues Verhalten und gute Zahlungsmoral.

Seite 59

China: Die digitale Diktatur

Keine traditionellen Werte mehr? Schöne Neue Welt! Das ist dann wohl der Paradigmenwechsel der Paradigmenwechsel. Die Welt wird Kopf stehen, aus den Fugen geraten und als buchstäblich «wertelose» Tyrannei rekonstruiert. Es ist wohl nicht übertrieben, wenn man dies als Sklaverei bezeichnet. Und das nicht nur aus ethischer, sondern auch aus technischer Sicht. China macht es vor. Dort arbeiten die Behörden an einem Punktesystem für jeden einzelnen Bürger. Da es im «Reich der Mitte» praktisch keinen wirksamen Datenschutz gibt, stehen der digitalen Tyrannei alle Wege offen. So werden alle Daten über ein Individuum aus allen Quellen zusammengezogen, seien es nun Behörden, das Internet oder Versandhäuser. Diese spielen sogar eine besondere Rolle: «Die Regierung arbeitet dabei unter anderem mit dem weltgrössten E-Commerce-Händler Alibaba zusammen, der offiziell als privat gilt und an der New Yorker Börse notiert ist. Die Behörden haben dabei auch Zugriff auf die Daten der Alibaba-Tochtergesellschaft Ant Financial, deren App Alipay mit rund 500 Millionen Kunden weltgrösster Anbieter für mobiles Bezahlen ist», berichtete die FAZ (online, 22.11.2017): «Bereits heute bewerten Internetkonzerne wie Alibaba und Tencent Käufe und Einträge ihrer Kunden und stellen eigenen Angaben zufolge die Daten dem Staat zur Verfügung.» Mit dem «Sozialen Bonitätssystem» wollen Partei und Regierung «eine zentrale Datenbank errichten, in der mithilfe grosser Datenmengen (Big Data) und Künstlicher Intelligenz sämtliches Verhalten von Unternehmen, Institutionen und Privatpersonen erfasst und bewertet werden soll.»

Abzug gibt es für oppositionelle Äusserungen oder für einen verschwenderischen Lebensstil.



Soziale Netzwerke beeinflussen den Status ebenfalls, denn Freunde mit schlechten Zahlen drücken auf den eigenen Wert.

Bis 2020 soll das System alle Bewohner Chinas erfassen. Bürger mit niedrigen Werten gelten dann als «unverantwortlich», nicht würdig Kredite, Hotelzimmer oder Reisegenehmigungen zu erhalten. Es droht die totale Sozialkontrolle.

Nach den Plänen der chinesischen Verwaltungszone Xiongan stuft das Bewertungssystem zum Beispiel «‚Geset-

zestreue, moralisches Wohlverhalten, soziales Engagement, Aktivitäten im öffentlichen Interesse und Umweltschutz' jedes einzelnen Bürgers» ein, zitierte die FAZ das Nachrichtenportal «The Paper». «Abweichungen von sozialen und moralischen Normen werden bestraft.» Sprich: Wer sich systemkonform verhält, bekommt mehr Punkte, wer sich an den gerade aktuellen Vorgaben «versündigt», bekommt Punkteabzug. «Regierungskritische Äusserungen» sollen ebenso mit «Punktabzug bestraft werden» wie erwachsene Kinder, «die ihre Eltern nicht regelmässig besuchen». Die Sanktionen reichen von Reiseverboten über die Sperrung von Bankkrediten und Kreditkarten bis hin zu «Freiheitsbeschränkungen».

Von der Überwachung zur Sklaverei

Die Überwachung kippt also in die Tyrannei – auch hier bei uns. Wenn man einmal ein anderes Datenprojekt betrachtet, wird einem das sofort klar: Nämlich anhand des allumfassenden elektronischen Zahlungsverkehrs und der Abschaffung des Bargeldes. Plastikkarten, PayPal und Banküberweisungen lassen sich staatlicherseits nun mal «leichter überwachen und sind dadurch natürlich die bevorzugten ‚Nachfolgeoptionen' auf dem Weg, Bargeld zu etwas ‚Verdächtigem zu machen'», hiess es auf der politischen Analyse-Website konjunktion.info (31.3.2015). Tatsache ist: Allein anhand unserer Online-Einkäufe lässt sich ein umfassendes Lebens- und Persönlichkeitsbild von uns zeichnen. Sollte das Bargeld tatsächlich verschwinden, würde jeder einzelne Zahlungsvorgang überwachbar. Und da fast alles im Leben Geld kostet, wäre unser Leben ohne Bargeld künftig wie ein offenes Buch.

Ja, aber: Ist es das nicht ohnehin schon? Durchaus. Aber die Durchleuchtung jedes einzelnen ist in diesem Fall noch nicht einmal das eigentliche Thema. Über die wirklichen Konsequenzen berichtet nämlich niemand: Ein ausschliesslich elektronisches Zahlungssystem wäre der Einstieg in die totale Sklaverei. Jedermann würde sofort auf den Knien herumrutschen, nur um wieder zahlen und sich ein Brötchen kaufen zu können. Wie war das noch in jenem alten dystopischen Spielfilm, bei dem es kein Bargeld mehr gibt und das gesamte Zahlungssystem nur noch auf einem computergestützten Punktesystem beruht? Der Titel des Films ist mir leider entfallen, und seltsamerweise wird er auch nicht wiederholt und kann man ihn nirgends mehr finden (sachdienliche Hinweise erbeten). Aber die Pointe ist mir noch lebhaft in Erinnerung: Als eine Familie aufgrund eines Verwaltungs- oder Computerfehlers längere Zeit keine «Zahlungspunkte» mehr zugeteilt bekam, lief der Familienvater irgendwann plötzlich ohne Arm herum. Um nicht zu verhungern, hatte die Familie das Körperteil amputiert und aufgegessen.

Digitale Zahlungsmittel gelten als schick, modern und «hip» und werden vom Mainstream wie z.B. dem City-of-London-Sprachrohr «Economist» gehypt, was das Zeug hält. Will man uns über Umwege eine digitale Währung schmackhaft machen, mit der anonyme Zahlungen ein Relikt der Vergangenheit wären?

Ausweg Blockchain?

Was kann man also tun? Als Hauptproblem des grossen globalen Überwachungssystems sehen viele die Zentralisierung: Riesige Monopole wie Google, Amazon und Facebook sammeln in ihren Rechenzentren enorme Datenmengen, die dann wieder von anderen, noch grösseren Zentralcomputern aufgesaugt werden, zum Beispiel bei «Sicherheitsbehörden». Sprich: von sogenannten «Knoten». Wieder andere sehen solche schädlichen Knoten in den Banken, die Währungen und Geldflüsse kontrollieren und manipulieren und alles über jeden wissen. Die einzige Lösung besteht für viele darin, eben diese Knoten aufzulösen, und den gesamten Datenverkehr über Millionen Computer dezentral zu organisieren, so dass kein einzelner Rechner alle Daten (zum Beispiel Nachrichten) besitzt, sondern sozusagen nur Puzzleteile. Und damit sind wir bei dem modernen Thema «Blockchain», das Prinzip, auf dem beispielsweise die «Kryptowährung» Bitcoin beruht. Dabei geht es darum, den Datenverkehr für Zahlungen, Produkte oder Inhalte neu zu organisieren und statt über Knoten über Millionen Rechner zu führen und gemeinsam zu verwalten. Egal, ob es sich dabei nun um Geld, Nachrichten, Texte oder andere Inhalte handelt. Klingt gut, finden Sie? Schon – aber auch dabei könnte es sich nur um eine Honigfalle der Tyrannei handeln, die zum Beispiel dafür sorgt, dass alle Welt auf digitale Währungen «fliegt» und das Bargeld mit der Zeit überflüssig – sprich: abgeschafft – wird. Was gleichbedeutend mit der Sklaverei wäre.

Freiheit ist Sklaverei, Sklaverei ist Freiheit

Nicht nur die Überwachung, auch die Versklavung funktioniert heute ja nicht über Zwang, sondern über Bedürfnisse, die künstlich erzeugt werden. Und das Bedürfnis nach Kryptowährungen wird geweckt – und wie: Digitale Zahlungsmittel gelten als schick, modern und «hip» und werden vom Mainstream gehypt, was das Zeug hält. Viele Medien sprachen in diesem Zusammenhang bereits von einem «Goldrausch». Die Kehrseite der Medaille heisst jedoch

➔

Seite 61

Überwachung und Versklavung. Das elektronische Geld zieht noch mehr Transaktionen in den bargeldlosen Bereich hinein. Misstrauisch sollte uns auch stimmen, dass der Erfinder des Bitcoin (und damit vermutlich auch der Entwickler der ersten einsatzbereiten Blockchain-Technologie) bis heute ein Phantom ist. Der Schöpfer der Währung, über die heute die ganze Welt redet, ist ein Niemand, der zwar einen Namen (Satoshi Nakamoto), aber keine Identität besitzt. Denn niemand weiss, wer sich hinter diesem Namen verbirgt:

Foto: FNDE (https://commons.wikimedia.org/wiki/File:-Dirk_M%C3%BCller_2012.jpg) https://creativecommons.org/licenses/by-sa/4.0/deed.en

«Ich bin auch der festen Überzeugung, und da mag man mir jetzt wieder Verschwörungstheorie vorwerfen, dass der Bitcoin nicht von irgendeinem anonymen Asiaten im Hinterzimmer zusammengeschraubt wurde», meinte dazu der populäre Börsenexperte Dirk Müller. «Aus meiner Sicht sind Kryptowährungen als neue Weltleitwährungen schon lange in der Vorbereitung – von denen, die auch heute schon dabei sind, unsere Gelder zu verwalten: von Zentralbanken.» Müller betrachtet die inzwischen vielen verschiedenen Kryptowährungen nur als «grossen Flächenversuch» und Marketinggag: «Hätte ich vor zehn Jahren gesagt: Wir schaffen das Bargeld ab und machen eine Kryptowährung, hätte man mich vom Hof gejagt» [4].

«Klasse, da sind wir reich geworden!»

Nach den Bitcoin-Versuchen würden die Leute wahrscheinlich anders reagieren: «Klasse, da sind wir schon einmal reich geworden!» Auch hier wird also ein Zwang in eine Nachfrage verwandelt. Mit anonymen Zahlungen habe das alles aber nichts zu tun, sondern die ersten diesbezüglichen Vorschläge von Zentralbanken drehten sich «um die totale Kontrolle» und darum, «jeden abklemmen» zu können, so Müller. Denn wie jede Technologie, kann auch diese für beides benutzt werden: zur Unterdrückung und zur Befreiung. Und wie bei jeder anderen neuen Technologie, werden Staaten und Geheimdienste davon wohl am wenigsten überrascht – und zwar weil sie direkt aus ihren Labors stammt. Wahrscheinlich ist also, dass all die Konzerne und Staaten mit ihren Etats und ihrer geballten Rechenpower auch diesmal einen Schritt voraus sein werden, um all die Schäflein, die mit ihrem Daten- und Zahlungsverkehr in die Blockchain-Technologie flüchten wollen, letztlich wieder aufzusammeln – ganz einfach, indem Staaten und Sicherheitsbehörden selber Blockchains «aufmachen». «Indizien weisen darauf hin, dass es sich bei Bitcoin um ein NSA-Programm handelt, um eine weltweite digitale Währung auf den Weg zu bringen», meldete das alternative Nachrichtenportal Natural News (12.10.2017). Und wie bei fast jeder Technologie auch, werden Militärs und Geheimdienste aufgrund ihrer finanziellen und technischen Möglichkeiten dabei führend sein:

Foto: Steve Jurvetson (https://commons.wikimedia.org/wiki/File:Jamie_Dimon,_CEO_of_JP-Morgan_Chase.jpg) https://creativecommons.org/licenses/by/2.0/deed.en

«Alle Kryptowährungen werden unter staatlicher Kontrolle sein», sagte einer, der es eigentlich wissen müsste, nämlich Jamie Dimon, Vorstandsvorsitzender der US-Bank JP Morgan Chase – also der grössten Bank der USA und der weltweit zweitgrössten Aktiengesellschaft überhaupt.

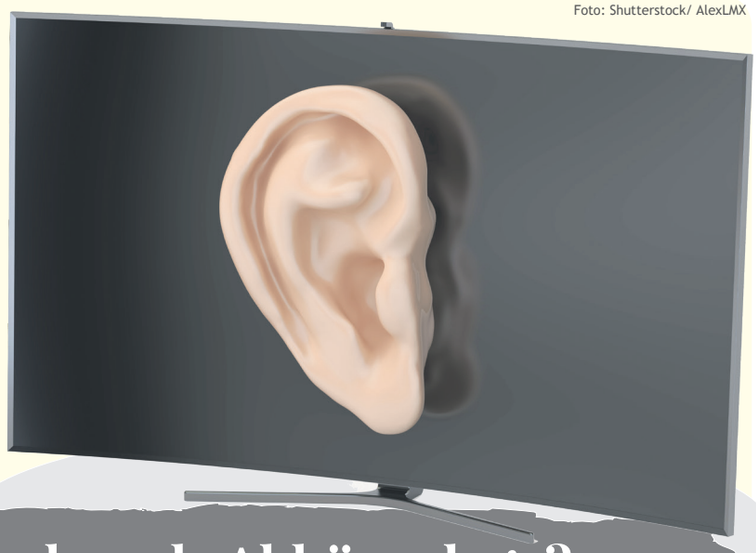
EINE BEVÖLKERUNG AUS SCHAFEN WIRD IMMER EINE REGIERUNG AUS WÖLFEN HERVORBRINGEN.

Edward R. Murrow

Quellen:

1. Die Welt, online, 2.5.2016
2. The Known Traveller - Unlocking the potential of digital identity for secure and seamless travel, World Economic Forum, Cologny/Geneva, Januar 2018
3. Macht steuert Wissen, 29.2.2016
4. youtube.com, Dirk Müller über Kryptowährungen über Bitcoin, 04.02.2018

Foto: Shutterstock/ AlexLMX



Der Fernseher als Abhöranlage?

Parker Higgins gehört zu den seltenen Menschen, die Endbenutzer-Lizenzverträge (EULA) und Datenschutzbestimmungen lesen. Was für die meisten wohl der langweiligste Lesestoff des Planeten ist, erinnert das Mitglied der Datenschutzorganisation Electronic Frontier Foundation (EFF) aber bisweilen an grosse Weltliteratur. An George Orwells Dystopie 1984, um genau zu sein.

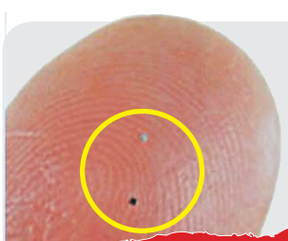
2015 hat Higgins die EULA für Samsungs neue Smart-TVs studiert und unter dem Stichwort «Spracherkennung» folgenden Satz gefunden: «Samsung könnte Sprachbefehle sammeln, um Ihnen Spracherkennungsfunktionen anzubieten und diese zu evaluieren und zu verbessern. Bitte beachten Sie, dass Ihre gesprochenen Worte, die persönliche oder andere sensible Informationen beinhalten, unter jenen Daten sein werden, die aufgenommen und an einen Drittanbieter übertragen werden, wenn Sie die Spracherkennung nutzen.» Solange das Mikrofon des Fernsehers im aktiven Modus ist, sollte man also im Wohnzimmer besser nichts allzu Intimes besprechen.

Dieser interessante Hinweis mag Literatur-Interessierten bekannt vorkommen: In Orwells Buch 1984 versucht der Protagonist Winston Smith gegen den Überwachungsstaat zu kämpfen. Darin ist zu lesen: «Jedes von Winston verursachte Geräusch, das über ein ganz leises Flüstern hinausging, wurde von ihm (Anm.: dem als «Televisor» bezeichneten Fernsehgerät) registriert. Ausserdem konnte Winston, solange er in dem von der Metallplatte beherrschten Sichtfeld blieb, nicht nur gehört, sondern auch gesehen werden. Es bestand natürlich keine Möglichkeit festzustellen, ob man in einem gegebenen Augenblick gerade überwacht wurde. Wie oft und nach welchem System die Gedankenpolizei sich in einen Privatapparat einschaltete, blieb der Mutmassung überlassen.»

Samsungs intelligente Fernseher hören in den Standardeinstellungen zumindest offiziell nicht permanent zu, was im Zimmer gesagt wird. Die Spracherkennung liesse sich sogar komplett ausschalten, wie der Lizenzvertrag versichert. Dazu hat Samsung auf Nachfrage von TechCrunch behauptet, dass es Such- und Sprachkommandos nicht über lange Zeiträume speichert oder an Dritte verkauft. Die Sprachkommandos werden zunächst in Text umgewandelt und damit maschinell verwertbar gemacht, danach werden sie auf Servern von Drittanbietern gespeichert. Was die Drittanbieter mit den erhaltenen Daten machen, sagt Samsung in dem Klarstellungs-Dokument jedoch nicht.

Deutlicher wird das in der deutschen Version der Datenschutzbestimmungen, die alle Abnehmer von Samsungs Smart-TVs akzeptieren müssen, bevor sie die Sprachsteuerung benutzen können. Der die Daten verwertende Drittanbieter ist die amerikanische Firma Nuance, die die Daten auf Servern in Irland sammelt und auch Apples digitale Assistentin Siri entwickelt hat. Die Sprachsteuerung von Samsung funktioniert derzeit nicht lokal, sondern immer cloudbasiert. Alle Kommandos nach dem initialen Startbefehl werden aufgenommen und an Nuances Server weitergeleitet, von denen sie ihr Feedback bekommen. Das gilt für Spielekonsolen, Smartphones, Amazons Echo, Smart-TVs, und alle anderen sprachgesteuerten Systeme in Haushaltsgeräten, Autos oder Unterhaltungselektronik. Trotz all der Bekenntnisse zum Datenschutz darf bezweifelt werden, ob die Audio-Aufnahmen bei den High-Tech-Konzernen wirklich in den besten Händen sind.

Quelle: zeit.de, Achtung, dieser Bildschirm hört mit, 26.02.2015



Zwei der winzigen Mikrochips auf einem Finger. Laut Zukunftsforscher Villani geht es aber «schon noch ein bisschen kleiner».

Werden wir bald mit Mini-Chips besprüht?

Für den Zukunftsforscher Oscar Villani ist der implantierte RFID-Chip «längst Schnee von gestern», denn Mikrochips können inzwischen so klein und günstig produziert werden, dass man sie zu tausenden an Menschen anheften könnte.

In einer ORF-Sendung aus dem Jahr 2014 versah Villani die Hand der Moderatorin Claudia Reiterer völlig unbemerkt mit hunderten fast unsichtbaren Mini-Chips. Die Chips sind dünner als ein Menschenhaar und mit blossem Auge kaum zu sehen. Laut Villani war dies aber nur der damalige Stand der Entwicklung und es ginge «schon noch ein bisschen kleiner.» Ausserdem lassen sich die Mikrochips auch nur allmählich abwaschen und bleiben bis zu zwei Wochen beim Träger.

Auf die Frage der Moderatorin, was man mit dem Chip so anstellen könne, antwortete Villani: «Ich hätte Ihnen damit eine Nummer verpasst. Das ist mal das mindeste, was ich tun kann. Und ich kann Sie damit rund um die ganze Welt verfolgen. In weiterer Folge könnte ich auch so Dinge wie Ihren Blutdruck messen, Ihren Zuckerhaushalt, paar biometrische Daten. Das ist schon drin.»

Villanis Fazit zum Stand der Überwachungstechnik deckt sich mit dem der vorliegenden Ausgabe: «Von den technischen Möglichkeiten her ist im Prinzip eine 24/7-Überwachung - ob das jetzt Kinder oder Erwachsene sind, ist eigentlich egal - auch schon jetzt möglich. In Zukunft halt noch unbemerkter, noch detaillierter. Das Nette daran ist: Eigentlich tun es ja immer mehr Menschen freiwillig.» Denn leider, stellte Villani konsterniert fest, hält der ethisch-moralische Fortschritt unserer Gesellschaft nicht mit dem technischen Fortschritt mit.

Quelle: ORF, Der gläserne Mensch

Mehr über die externe Steuerung von Autos ab Seite 37

Autos von Regierungskritikern im Visier der CIA-Hacker? - Der Fall Michael Hastings

Vieles spricht dafür, dass der kritische Journalist Michael Hastings Opfer einer Hacker-Attacke wurde, als sein Mercedes mit 165 km/h in eine Palme raste und abbrannte. Der Verdacht eines Cyber-Angriffs wurde sogar durch Aussagen eines ehemaligen Funktionärs der Bush-Administration untermauert. Mehr Technologie ist eben nicht immer gleich mehr Sicherheit. In Hastings Fall garantierte sein modernes Auto möglicherweise nicht seine Sicherheit, sondern die Job-Sicherheit hochrangiger Militärs, denen er ein Dorn im Auge war.

Juni 2013, ein brennender Unfallwagen im nächtlichen Los Angeles. Ein Mercedes als Trümmerhaufen, Ursache unklar, keine Zeugen. In den Flammen stirbt der US-Journalist Michael Hastings. Er recherchierte gerade an einer neuen Enthüllung. Seine letzte Story hatte einen Elite-General die Militärkarriere gekostet: Durch einen Artikel im US-Magazin «Rolling Stone» hatte er den Rücktritt des Kommandeurs der NATO-Truppen in Afghanistan General Stanley McChrystal bewirkt und war zum Zeitpunkt seines Todes mit einem Artikel über CIA-Chef John Brennan befasst. Er starb, weil sein Mercedes nachts auf menschenleerer Strasse mit mehr als 165 km/h in einen Baum raste und dreimal explodierte. Kurz vor seinem Tod hatte Hastings Kollegen und Wikileaks darüber informiert, dass er befürchte, dass sein Auto manipuliert worden sei, dass das FBI ihn verfolge und er untertauchen müsse. Richard Clarke, der ehemalige Terrorabwehrkoordinator der USA sagte, Hastings Todesumstände trügen alle Merkmale eines Cyberangriffes auf sein Auto.

Clarke, der für Ronald Reagans, Bill Clintons und George Bushs Administrationen gearbeitet hatte, sagte über Hastings Unfall, er sei «übereinstimmend mit einer Cyber-Attacke». Clarke meinte, es gäbe keinen Grund zu glauben, dass Geheimdienste von Supermächten wie den USA nicht wüssten, wie man die Kontrolle über ein modernes Auto gewinnt. «Was als Resultat einiger Universitätsforschungen enthüllt wurde, ist, dass es relativ einfach ist, dich in das Kontrollsystem eines Autos zu hacken; Dinge zu tun, wie die Geschwindigkeit zu erhöhen, wenn der Fahrer die Geschwindigkeit nicht erhöhen will; oder die Bremsen zu aktivieren, wenn der Fahrer nicht bremsen will oder ein Air Bag auszulösen», sagte Clarke der Huffington Post. «Man kann heute wirklich destruktive Dinge machen [...] und es ist nicht besonders schwer.»

Cyber-Attacke kaum nachvollziehbar

Wenn es Falle Hastings zu einer Cyber-Attacke gekommen wäre, wäre der Täter laut Clarke «wahrscheinlich damit durchgekommen.» So eine Manipulation sei fast unmöglich nachvollziehbar, selbst wenn wie bei Hastings Unfall nicht alle Computer an Bord des Autos geschmolzen wären.

Die Polizei hatte einen digitalen Angriff auf Hastings Vehikel von Anfang an ausgeschlossen, doch laut Clarke hat die US-Polizei sowieso nicht die Expertise für solcherlei Ermittlungen: «Ich denke, man bräuchte die allerbesten Leute der US-Geheimdienstwelt und der Strafverfolgung, um etwas zu entdecken.» Hastings fuhr einen Mercedes C250 Coupé, als er um 04:30 nachts in einen Baum raste. Ein Online-Video zeigt das demolierte Auto in Flammen.

Richard Clarke, der ehemalige Terrorabwehrkoordinator der USA, hält eine Hacker-Attacke in Hastings Fall für realistisch, jedoch schwer beweisbar.

Foto: Aude (https://commons.wikimedia.org/wiki/File:Richard_clarke.jpg) https://creativecommons.org/licenses/by-sa/3.0/deed.en

«Ich bin kein Verschwörungstheoretiker. Tatsächlich habe ich den grössten Teil meines Lebens damit verbracht, Verschwörungstheorien zu entkräften», so Clarke, der in Konflikt mit der zweiten Bush-Administration geriet, als er die Entscheidung, den Irak anzugreifen, kritisierte. «Doch meine Regel war immer, eine Verschwörungstheorie nicht anzugreifen, bis ich sie widerlegen kann. Und im Falle von Michael Hastings, stimmen die Beweise mit einer Cyber-Attacke überein. Das Problem ist, dass man es nicht beweisen kann.»

Wikileaks hat 2017 Dokumente veröffentlicht, die zeigen, dass die CIA ab 2014 systematisch damit beschäftigt war, die Software von Autos zu manipulieren, um Mordanschläge verüben zu können.

Die 2017 von Wikileaks veröffentlichten Vault-7-Dokumente beweisen, dass die CIA mit Forschungen zur Kontrollübernahme von Bordcomputern beschäftigt war. Dass der Geheimdienst in der Lage ist, ein Gefährt zu hacken, ist sehr wahrscheinlich.

Quelle: huffingtonpost.com, Was Michael Hastings' Car Hacked? Richard Clarke Says It's Possible, 26.06.2013